La paradigme téléphonique

Christophe Chalons, université Paris7, équipe de logique mathématique

May 10, 2014

Introduction

0.0.1 Table des matières commentée

Le premier chapitre traite du lemme de l'étoile. Il jouera un rôle surprenant dans la dualité des degrés ludiques. Il est équivalent à l'axiome du choix et de type (au sens informatique) $((A \to B) \to A) \to A$ qui est l'axiome de Pearce (schéma d'axiome qu'il suffit de rajouter à la logique intuitionniste pour obtenir la logique classique). Ce n'est qu'une reformulation du procédé diagonal sans le << 2 >>.

Le deuxième chapitre entre dans le vif du sujet: les degrés ludiques. C'est un chapitre de définitions et de lemmes qui permettent de visualiser, tant que faire se peut, le décor. La fin du chapitre aborde le surprenant théorème << nonTSD=multitable>> (qui exprime comment récupérer la localité des stratégies pour réaliser le miracle d 'implémenter des téléphones non locaux (mais nonTSD!), avec un prix (cher) payé qui est de rendre le monde multiple et le succès attendu seulement dans quelques mondes). TSD veut dire *transmettre signal à distance*

En toute fin de chapitre, nous donnons quelques interprétations possibles, sans nous attarder. Nous tentons aussi d'aider le lecteur à aborder des exemples concrets de téléphones

Le troisième chapitre situe quelques objets déjà connus, qui sont des degrés ludiques très particuliers. Quand un téléphone d'uplicité2 a un de ses combinés sans écran et l'autre sans clavier (cardinal 1 des supports concernés), il se comporte comme ce que nous avons appelé *un téléphone de Tukey*. Or il se trouve que les degrés de Tukey sont connus et ont été étudiés. Nous en proposons cependant une étude systématique pour ce qui concerne les lemmes techniques de base, afin de les re-situer dans le contexte téléphonique (ils n'ont pas été présentés historiquement comme tels).

Le quatrième chapitre est un chapitre d'exemples qui nous avaient retenus au début. Certains lecteurs trouvaient ce que certains d'entre eux illustraient bien le slogan *mesurer de la magie* (sans pour autant, par essence, en connaître les ficelles)

Au chapitre 5 nous donnons la seule preuve connue selon nous de l'indéterminisme reproductible de la Nature. Il s'agit d'une preuve irréfutable (à ne pas confondre avec des preuves <<intra-formalisme>> qui viennent à l'intérieur d'une modélisation et ne sont pas irréfutables pour qui rejette la modélisation). Malgré le côté <<ronflant>> de cette expression, il ne s'agit pas d'une preuve ingénieuse ou difficile, mais d'un simple exercice pour étudiant dont le principe est évidemment bien connu. Nous y donnons aussi une preuve (avec le même statut) de l'impossibilité de cloner certaines entités matérielles (idem, irréfutables et non pas intra-modélisation). Ces preuves continueront de s'appliquer même si la physique change. Elles ne s'appuient que sur des prédictions concrètes et déjà testées de la théorie quantique et non sur la théorie elle-même. Nous donnons aussi dans ce chapitre des exemples de téléphones FMQ.

La chapitre 6 est consacré à l'éternité. La notion est détaillée et définie dans le chapitre. Nous y démontrons l'importance des ordinaux et on espère que l'économie de pensée et la richesse conceptuelle apportée par les degrés de Tukey s'y voit bien.

Le chapitre 7 est consacré à un théorème qui nous tient grandement à coeur. Il met selon nous un terme à toute possibilité (que certains caressent de leurs voeux) de trouver de manière éventuellement détournée des interprétations << au moins un peu locales, même si pas complètement >> du fonctionnement des téléphones FMQ. De plus, le théorème principal démontre l'impossibilité, pour l'approche probabiliste de saisir le mécanisme naturel à l'origine de l'existence des FMQ (les probabilités ne peuvent pas descendre sous les casino-inoffensifs définis un peu plus loin). Le théorème du chapitre dit que tout degré ludique d'uplicité 2 non trivial est Tukey-offensif.

Le chapitre 8 est consacré à 6 théorèmes techniques concernant des classes faibles de degrés ludiques. Il classifie une partie des puissances ludiques très faibles. On y voit en particulier à quel point les FMQ sont, bien que non locaux, très faibles. Les chapitres 7 et 8 s'opposent dans leur morale en quelque sorte. L'un dit la force et l'autre dit la faiblesse des degrés FMQ (entre autre). Au chpitre8 est démontré qu'à condition d'admettre une conjecture de Connes et Kirchberg, l'ensemble des degrés ludiques FMQ de support fini est récursif (et peut donc être calculé par un algorithme).

Le dernier chapitre, une sorte d'annexe, démontre qu'il existe une distinction clinique entre vrai hasard et faux hasard, même à comportements statistiques égaux de leurs productions respectives. Il utilise l'axiome du choix, mais donne une conclusion de principe.

0.0.2 Motivations

Ce texte plus formel est la rédaction <<au propre>> de ma page internet de 1998 appelée <<degrés ludiques>>. Nous avons extrait d'un texte de 300 pages environ qui formalisait ce que j'avais appelé le paradigme téléphonique[1], et comment il génère des questions et parfois des réponses à des questions réputées informalisables, une des 5 parties. Celle concernant les degrés ludiques, comment dire <<à froid>>, sans surcouche philosophique ou théorèmes périphériques[2]. Cet extrait l'a été avec comme spécification de tenter de lui donner un format de type thèse (qui exclut donc une écriture trop fantaisiste, des prises de position, des questions ouvertes trop nombreuses dans le corps du texte, etc). Nous revenons quand-même dans cette sous-section intitulée *motivations* sur la façon dont ces questions se sont d'abord posées naïvement et sans préoccupation mathématique, puis se sont précisées avec le souci de ne pas travestir la problématique initiale lors du processus de formalisation, en particulier d'éviter le piège de la modélisation (une modélisation (excessive) rend forcément douteuse << ses conlusions exportée d'elles >> au moment du retour à la préoccupation initiale).

Nous sommes depuis toujours et presque à chaque instant de nos vies confrontés à une difficulté de type physique qui est de formaliser la possibilité de survenue d'évènements qui paraissent peu possibles (ou plus exactement d'en mesurer les degrés d'"impossibilité" ou de "paradoxalité""):

- Notre aptitude à gagner au jeu <<antipointfixe>> (voir la définition ci-dessous), aptitude qui ne fait aucun doute pour nous, nous la <<prouvons matériellement>> des dizaines de fois chaque jour
- Notre aptitude à <<faire des mathématiques>> d'une manière différente de ce qu'on attendrait de la façon d'en faire de la part d'un ordinateur
- De nombreuses <<surprises>> ou comment dire <<prodiges physiques>> qui ne peuvent être que qualifiés de cadeaux de la nature (dans une acception neutre du terme)

[1] le texte complet sera mis sur HAL en plusieurs morceaux

[2] Le choix de l'extrait n'est pas de mon fait, mais de lecteurs désireux de sélectionner les résultats les plus directement en lien avec les degrés ludiques avec la contrainte de ne pas dépasser la centaine de pages

Cela va même un peu plus loin, dans la mesure où on a le sentiment de pouvoir démontrer mathématiquement (c'est à dire irréfutablement) que tel ou tel de ces évènements sont réellement impossibles. Comme exemple, pratiquement record, on peut signaler les expériences qui ont donné naissance à la théorie quantique, affinées, jusqu'à aboutir à des formes les plus spectaculaires possibles que sont les confirmations expérimentales du théorème de Kochen Specker. En voici des exemples:

- On peut <<colorier quantiquement>> la sphère S_3 avec 4 couleurs (la sphère S_3 ne peut pas être coloriée avec 4 couleurs). Autrement dit, il existe un appareil dont le format est de ressembler à un téléphone, qui comporte 2 combinés. Chaque combinés comporte un clavier et un écran. La clavier $\mathbb{R}^4$ (on le suppose muni de sa structure euclidienne canonique. On regarde de plus $\mathbb{R}^4$ comme l'ensemble des quaternions). L'écran est $4 := \{0, 1, 2, 3\}$ pour chaque combiné. Les combinés ont une utilisation unique et cette utilisation peut être <<n'importe quand>>, et à des dates aussi différentes (ou <<simultanées>>) que l'on veut, en des endroits aussi différents que l'on veut l'un de l'autre. La garantie est que si on tape les éléments u, v sur les claviers alors les i, j qui s'afficheront sur les écrans sont tels que $non(u_i \perp v_j)$ et si $u = v$ alors $i = j$ où ici $u_0 := u; u_1 := u\times$ le quaternion u; $u_2 := u \times j$ et $u_3 := u \times k$.

- Exemple dû à R.Penrose: cette fois-ci, les claviers sont tous les deux $3 := \{0; 1; 2\}$. Les écrans sont tous deux l'ensemble des applications de 3 dans $\mathbb{Z}/2\mathbb{Z}$. La garantie offerte est que quelles que soient les dates d'appui sur les touches respectives x, y, et quels que soient les emplacements des combinés, s'afficheront sur les écrans des éléments u, v tels que $\sum u_i = 0$ et $\sum v_i = 1$ et $u_x = v_y$. On laisse le lecteur voir que le présent téléphone ne peut réussir ce prodige sans que ses combinés ne communiquent l'un avec l'autre pour ça. **Cependant, il y a un saut absolument énorme** entre le fait qu'ils le fassent et le fait qu'on puisse, en les considérant comme boites noires, exploiter qu'il le fassent pour, nous, utilisateurs, <<s'envoyer quelque chose>> à distance.

Le théorème de Kochen Specker affirme que dans le cas général, des dispositifs dont la théorie quantique abstraite prévoit la fabricabilité, ne peuvent être conçu comme ayant des combinés se comportant de manière indépendante. C'est sous le vocable de *non localité* qu'on réfère à ce paradoxe.

Il dit que pour tout espace vectoriel de dimension finie ≥ 3 sur $\mathbb{C}$, la plupart des garanties téléphoniques (les définitions formelles sont données plus loin) de la forme suivantes sont non locales, où f est une forme bilinéaire non nulle: *l'ensemble des* $((baseortho_1, i), (baseortho_2, j))$ *telles que l'image par* f *du couple formé de l'élément* i *de* $baseortho_1$ *et de l'élément* j *de* $baseortho_2$ *est non nulle*

Bien que motivé par cette problématique physique centrale, la suite du texte n'est constitué exclusivement que d'affirmations mathématiques. Nous n'entrons aucunement dans la physique.

Le jeu <<antipointfixe>>

Il s'agit du jeu suivant, à la fois extrêmement idiot en apparence, mais extrêmement significatif: Léa joue D'ABORD un élément $x \in [0; 100]$. Puis Bob a presque tout son temps pour répondre et, voyant le x joué par Léa, doit proposer $y \in [0; 100]$ tel que $|x - y| > 10$.

Aucun être humain ne doute, qu'à la place de Bob, il gagnera à ce jeu. Pourtant, aucun être humain ne peut prétendre être une application **discontinue** de $[0; 100]$ dans $[0; 100]$, lesquelles applications discontinues sont les seules stratégies gagnantes possibles à ce jeu. A noter qu'ici il n'y a aucun piège ni aucun parasite qui viendrait travestir, dans le cheminement formalisant, la question de fond qui est derrière: afin de ne pas gêner Bob dans la vue de x, Léa peut et doit être conçue comme jouant sur un écran coloré $[0;100]^2$ une <<coloration>> de l'écran définie par $(u,v) \mapsto noir$ quand $u < x$ et $(u,v) \mapsto blanc$ quand $u \geq x$ de sorte que Bob est conçu comme <<voyant bien>> le x joué par Léa.

Les 3 <<grandes options>>

Face à la question précédente, si nous interrogeons les scientifiques et plus généralement les <<gens qui comprennent bien la question>>, on obtient 3 grandes catégories de propositions face à la question soulevée:

- La première est qu'il existerait réellement un x face auquel Bob perdrait, hésiterait éternellement, et finalement choisirait un y qui serait ... égal à x
- La deuxième est que Bob, inconsciemment, utilise une fonction discontinue gagnante pour jouer son y en fonction du x imposé par Léa
- La troisième, la plus répandue chez la plupart des physiciens, est qu'à l'instar de la nature elle-même, Bob n'est pas déterministe et n'a pas besoin d'utiliser une fonction discontinue pour <<gagner quand-même>>, pas plus que la souris d'un pc de bureau qui parvient à renvoyer à chaque instant une position qui est un élément de $A := \mathbb{N}^2 \cap [0;2000]^2$, offrant l'illusion de réaliser <<l'impossible>> implémentation d'une application (forcément discontinue!!!) de $B := [0,2000]^2$ dans telle que $\forall x \in B : dist(x, f(x)) \leq 0.1mm$

Il est à noter que la troisième position philosophique se légitimise opportunément en se servant de la révolution physique du début du 20ième siècle, mais que n'aurait-on pas reproché aux physiciens des siècles précédents de proposer une <<non-explication>> de ce genre?

Impossibilité de trancher

Il n'y a pas besoin de longues explications pour s'apercevoir que le problème précédent n'offre pas de prise. Il nous place devant deux faits: le premier étant le théorème des valeurs intermédiaires enseigné dès les premières années de faculté, le deuxième étant notre aptitude à réussir ce qu'une fonction continue ne réussit pas, sans pour autant avoir au niveau du conscient la sensation que nous mettons en branle une fonction discontinue pour gagner à un jeu pourtant trivial.

Difficulté transportée

Fort heureusement, la <<révolution quantique>> (qui s'est quelque peu opérée dans la douleur au début du vingtième siècle) a apporté avec elle son lot de <<prodiges>> directement réalisés par la nature indépendamment d'une interface humaine <<gagnant à un jeu simple>>. Les <<prodiges>> les plus aboutis sont les différentes confirmations du théorème de Kochen Specker, confirmations qui sont directes et ne nécessitent pas de phase de modélisation, ni de statistiques (contrairement à la plupart des prédictions théoriques dites confirmées, pour lesquelles cette notion de confirmation n'est qu'un abus de langage destiné à la vulgarisation)

L'intérêt du théorème de KS et de ses confirmations directes[3] et reproductibles est qu'ils n'offrent strictement aucune porte de sortie dite <<classique>>, enparticulier pas d'interprétation "réaliste" purement locale. Il est donc vain de chercher une interprétation de la physique quantique, une sorte d'explication, aussi folle soit-elle, qui réconcilierait la physique avec les mathématiques, du moins avec la partie dite <<irréfutable>> des mathématiques, à savoir ce qu'elles admettent comme <<axiomes logiques>>. Evidemment, il va sans dire, que nous excluons dans ce propos les interprétations dites <<multimonde>>, que trop peu de professionnels accepteraient de qualifier de <<classique>>. Il est évident que la théorie physique est <<consistante>> avec l'idée de <<multimonde>>. De la même manière que toute tautologie cesse d'en être une si on indice les occurrences de ses variables propositionnelles par des numéros différents pour chacune. Si notre préférence est en faveur d'une approche multimonde du réel, nous n'en parlons cependant pas dans la suite du texte, en dehors du fait que l'on peut considérer cette préférence comme une motivation des théorèmes principaux (nonTSD=multitable, etc) de la suite.

Contenu du travail

L'objectif du texte qui suit est d'étudier en détail ce que nous avons appelé *réduction ludique*, qui n'est rien d'autre que l'ordre partiel naturel que l'on peut mettre entre <<différents prodiges>> de sorte que $X \leq Y$ signifie *si on dispose du <<pouvoir>> d'obtenir le prodige Y alors on dispose <<mécaniquement>> du prodige X*

La définition formelle est donnée dans le texte, nous ne la reproduisons pas ici. Une partie du travail a consisté à revenir sur la notion de degré de Tukey, vu comme mesurant la puissance d'un téléphone. En effet, les degrés de Tukey sont des cas très particuliers de degrés ludiques (ceux d'uplicité 2 où leclavier de l'un est de cardinal 1 et l'écran de l'autre est de cardinal 1, ce qui impose aux utilisateurs de se concevoir comme émetteur ou récepteur), mais ils ont l'avantage d'avoir fait l'objet d'études sérieuses depuis une moitié de siècle. Les voir comme des puissances de téléphones permet de réaliser qu'ils généralisent les cardinaux. Ils permettent aussi d'étudier une différence entre deux infinis qualitatifs (celui auquel nous sommes habitués, disons <<dans l'avenir>> et l'infini <<vers le passé>>, qui a une nature différente). Les degrés de Tukey mesurent la quantité d'information (attention, ce n'est pas la notion de Shannon).

Il n'y a presque pas de considérations physiques dans la suite car nous sommes tout occupés à étudier en détails les degrés ludiques (en particulier à établir les lemmes triviaux mais qui <<posent>> le paysage). On espère gagner une étude assez détaillée de ce que veut dire "jouer"' de manière très générale et en amont des théories des jeux de l'économie ou des jeux à information parfaite de la logique professionnelle. Nous utilisons l'expression <<*en amont*>> parce que ce qui nous intéresse n'est pas l'optimisation pratique de stratégies, **mais leur simple existence.** Insistons en effet que tout couple de joueur jouant classiquement qui voudrait réussir la garantie particulière offerte par KS (note de bas de page) serait tel que ses membres **seraient obligés de communiquer**, et on peut le prouver (c'est l'affirmation du théorème qui dit que toute garantie ludique qui est graphe d'une fonction est TSD). L'inexistence prouvable d'une stratégie à un jeu pourtant constaté <<gagné par la nature>> nous interroge au préalable sur l'existence de stratégies et sur leur nature, avant de chercher l'optimisation. Les mathématiques nous imposent le théorème de Gales Stewart (les jeux à information parfaites, à deux joueurs, de longueur finis (pour faire simple) sont

[3] L'expérience GHZ par exemple. Plus récemment, la prédiction d'un téléphone à deux combinés garantissant le <<prodige>> suivant: le clavier de chaque combiné est l'ensemble $3 := \{0; 1; 2\}$ et son écran est l'ensemble des applications de 3 dans $\mathbb{Z}/2\mathbb{Z}$. La garantie offerte est que quelles que soient les dates d'appui sur les touches respectives x, y, et quels que soient les emplacements des combinés, s'afficheront sur les écrans des éléments u, v tels que $\sum u_i = 0$ et $\sum v_i = 1$ et $u_x = v_y$

déterminés). Elles nous imposent aussi l'indétermination des jeux à trois joueurs ou plus (théorème ci-dessous). Une réflexion sur ces jeux montre que peut-être la notion de stratégie n'est-elle pas ce qu'on imagine. En effet, en un certain sens, nous pensons que **les jeux à information parfaite à un nombre quelconque de joueurs DEVRAIENT être déterminés, quitte à changer la notion de stratégie habituellement considérée**

Théorème 1 *Il existe* $\phi_1 \in (((2 \times 2) \to 2) \times (2 \to 2)) \to 2; \phi_2 \in (2 \times ((2 \times 2) \to 2)) \to 2; \phi_3 \in (2 \times (2 \to 2)) \to 2$ *telles que pour toutes* (a, f, g) *avec* $a \in 2, f \in (2 \to 2)$ *et* $g \in (2 \times 2) \to 2$, *il n'est pas vrai que* $a = \phi_1(f, g)$ *et* $f(a) = \phi_2(a, g)$ *et* $g(a, f(a)) = \phi_3(a, f)$

Les <<prodiges>> reproductibles de la théorie quantique nous imposent les mêmes interrogations. L'être humain sera-t-il capable un jour, parce qu'il aura mieux compris ce que veut dire *façon de jouer* de réussir, en couple, sans que les alliés ne communiquent de quelque façon que ce soit, à garantir des protocoles tels que la Nature les offre selon KS? Une chose est sûre, ces *façons de jouer* ne seront ni des fonctions définies sur des input à valeurs dans des ensembles de <<coups çà jouer>>, ni, comme on pourrait l'imaginer dans le cas **très particulier et trop pauvre** du jeu antipoint fixe, des fonctions qui utiliseraient un <<random>> donné par la nature. Ce dernier point est prouvé au chapitre où nous démontrons que tout degré ludique est Tukey-offensif. En dessous des degrés que nous avons nommés *casino-inoffensif*, même une vision probabiliste ne distingue plus rien te collapse tout. Pour donner une image concrète de ce que ceci signifie, imaginons **un nombre fini** de boites fermées. Léa a le droit d'ouvrir certaines boites mais pas toutes. Puis elle doit deviner une information sur le contenu de la boite fermée. Etoffons la règle en admettant que Bob connait le contenu des boites mais ne peut envoyer à Léa que certains types et niveaux d'information. C'est un exercice classique de prouver qu'il n'existe aucune stratégie pour Léa qui lui permette de faire mieux en ouvrant des boites que ce qu'elle est capable de faire, à l'aide de Bob, **avec une seule boite** dans le jeu. Ici la théorie de la mesure et les probabilités ne peuvent plus rendre compte de très petit supplément qu'offre d'ouvrir d'autre boite que celle sur laquelle on parie. Notons qu'en présence de l'infini, (ie admettre une infinité de boites) le phénomène change du tout au tout. Mais **même avec seulement un nombre fini de boites**, remplacer la notion d'information <<habituelle>> par celle de degré de Tukey change aussi la donne et permet d'analyser le phénomène plus finement. Finalement, il nous fallait un outil pour mesurer toutes les magies possibles et imaginables, même si parfois complètement fictives. Nous nous sommes concentrés à seulement l'introduire.

L'outil pour mesurer cette magie est qualitatif. Il en émerge par contre-coup un éclairage sur les interprétations possibles de la physique quantique. Certaines nous semblent devenir nettement moins raisonnables (en fait falsifiée comme nous le verrons), d'autres seraient plutôt "confirmées".

Les théorèmes essentiels sont les suivants:

- Tout degré ludique d'uplicité finie qui est TSD est multitable. Ce qui signifie que si on renonce à une hypothèse <<unimonde>>, la seule hypothèse que la Nature ne nous offre pas de <<téléphones>> permettant d'envoyer au moins un bit à distance entraine qu'il n'existe aucune expérience reproductible aussi astucieuse soit-il qui permette de violer la localité <<multi>> (un téléphone est multitable quand il possède une stratégie LOCALE ... mais <<multimondique>> en quelque sorte qui lui permet de réaliser sa garantie téléphonique sur au moins une table)
- Les ordinaux suffisent en un sens très absolu à étudier la notion <<d'éternité>> (qui est une notion un tout petit peu différente de l'infini, généralement conçu comme un *infini dans l'avenir*)

- Il y a un incroyable espace entre le local et la puissance qui permet de transmettre au moins un bit à distance. Dans cet espace vivent toutes les nuances permettant de formaliser *l'indéterminisme vrai* de Natures supposées. Le chapitre ??? étudie en détail ces différents niveaux

- Les probabilités constituent une approche drastiquement limitée et imparfaite pour <<comprendre>> un objet naturel non déterministe. En effet, il existe une très large classe de téléphones non triviaux qui sont pourtant ce que nous avons appelé *casino-inoffensifs*. Ce sont des téléphones que les probabilités ne distinguent pas des triviaux sur *le plan clinique*. Pourtant un des théorèmes les plus importants de la présente thèse est que **tout degré ludique non trivial d'uplicité 2 est TUKEY-Offensif**. Autrement dit, en dehors des téléphones en plastique pour enfant, **tout téléphone** permet d'augmenter le niveau d'information envoyé. Or sous la barre des casino-inoffensifs, l'approche probabiliste écrase et ne voit donc pas ce supplément d'information. Cela démontre aussi que la non localité quantique est **reproductiblement concrète**

Globalement, nous présentons dans ce texte un outil automatisant la recherche de problèmes réputés *invisibles* par l'approche mathématique. Il s'agit de la réduction ludique (qui est une formalisation de ce que nous avons appelé le paradigme téléphonique). Comme dit ci-dessus, elle permet de distinguer des états qui étaient considérés habituellement comme indiscernables, par exemple, une ignorance de conditions initiales conduisant à calculer des probabilités faute de mieux vs une situation où l'état est réellement libre d'agir comme il veut, **mais suit les mêmes statistiques que le précédent**. Elle classe aussi dans un ordre partielle les puissances <<téléphoniques>>.

Sur le fond, ce travail a été mené pour l'essentiel en 1997 et il a été publié alors sur mon site internet en 1999([Cha1]). Les idées principales ont été reprises, avec un angle de vue légèrement différents, dans [C.R.]. Je remercie les grands esprits altruistes qui m'ont harcelé pour que je lui donne une forme acceptable et le ré écrive en thèse de doctorat afin de lui donner un meilleur label et une publication officielle. J'espère y être arrivé. Cette thèse parle de relations sur les relations. Plus précisément, elle introduit une nouvelle manière de classifier les relations, qui prolonge la comparaison de Tukey. Elle entraîne alors un nouveau regard sur la comparaison de Tukey.

Nous n'avons pas inclus dans cet extrait de nombreuses suites, disons <<encore instables>> selon les lecteurs qui ont choisi de ne retenir que le présent contenu pour un format thèse, mais qui ont toutes été produites avec les mêmes motivations <<téléphoniques>>[4]. Pour certaines, elles ont été déjà publiées avec un regard extérieur dans [C.R.] (un journal d'arithmétique faible, avec une insistance sur la thématique de la réduction de Turing plus appuyée)). D'autres l'ont été par moi-même au CRAS (les théorèmes de la cible). Enfin, le mail que j'avais envoyé en 1998 à la mailing list des théoriciens des ensembles a été détaillé et publié par Joel Hamkin, puis il a développé cette partie du paradigme et publié d'autres travaux ensuite de sorte qu'il n'est pas utile d'inclure ici de supplément << version théorie des ensembles>> puisqu'ils peuvent être trouvés, développés avec des regards différents dans des travaux ultérieurs. Le seule partie qui n'avait, hélas, jamais été reprise (le texte internet de 1998 était vraiment irrespectueux pour les lecteurs) est la présente (celle définissant et décrivant les degrés ludiques).

Par relation, nous entendons un triplet (E, F, R), où E, F sont des ensembles et R une partie de $E \times F$.

[4]même si plusieurs interlocuteurs me disent qu'ils n'aiment pas ce terme, j'y tiens, je n'en trouve pas d'autre qui soit adapté à la démarche et la copie que je mets sur HAL est titrée *paradigme téléphonique*

Dans tout le texte qui suit, quand on parlera d'une relation (E, F, R) il sera toujours supposé implicitement que:

$$E \textbf{ est non vide et } F \textbf{ est non vide.}$$

.

En effet, le paradigme téléphonique est incompatible, dans sa spécification, avec des claviers ou des écrans vides. La possibilité de comprendre le rôle de l'ensemble vide nous semble une question pour l'instant ouverte. Essentiellement, dans la suite, les ensembles (on travaille dans ZFC) sont là pour *pouvoir parler*. Mais une garantie téléphonique doit se concevoir comme une relation définie sur l'univers entier. Si les degrés peuvent être canoniquement définis, les relations elles-mêmes ne peuvent pas avoir de définition $DEFAULT$ quand les inputs ne s)ont pas dans les supports. Quelque convention qu'on choisisse, on obtient des $DEFAULT$ contradictoires.

Table des matières

Chapitre 1

Lemme de l'étoile
Introduction au degrés Ludiques

Le lemme suivant va fonder la dualité des degrés ludiques. Il s'agit du théorème de Cantor généralisé à d'autres ensembles que le seul ensemble $2 := \{0; 1\}$. Son profil, à savoir la signature $((A \to B) \to A) \to A$ est l'axiome (appelé *axiome de Pearce*) qu'il suffit de rajouter à la logique mnimale pour obtenir la logique classique.

Lemme 2 *Soient E,F deux ensembles. Soit L une application de F^E dans E. Alors il existe $e \in E$ tel que pour tout $y \in F$ il existe $f \in F^E$ telle que:* $[f(e) = y$ *et* $L(f) = e]$

Preuve : Supposons que pour tout $e \in E$ il existe $f(e) \in F$ tel que pour toute $g \in F^E$ $L(g) \neq e$ ou $g(e) \neq f(e)$. Alors en particulier, $L(f) \neq L(f)$ ou $f(L(f)) \neq f(L(f))$ ce qui est contradictoire

Remarque : Nous avons associé (avec l'axiome du choix) à chaque élément de $(E \to F) \to E$ certain(s) éléments privilégiés de E. Dans la suite le théorème de l'étoile jouera un rôle assez typique dans la **dualité des degrés ludiques**.

Les sections suivantes entrent dans le détail de ce lemme, en étudient quelques généralisatins légères et le situent au sein de ZF.

1.1 Statut du lemme de l'étoile dans ZF

La forme propositionnelle $((E \to F) \to E) \to E$ est le schéma d'axiomes qu'il suffit de rajouter à la logique intuitionniste pour obtenir la logique classique.

Cependant cette coincidence de forme est probablement l'indice de quelque chose en relation avec la correspondance de Curry Howard, qui ne sera hélas pas développé dans la suite du texte. Une des versions rapidement équivalentes au théorème de Brouwer nous offre la même coincidence, que nous énonçons volontairement sous forme abstraite:

Théorème 3 *Pour des ensembles structurés convenablement A, B, pour toute application L de $A \to B$ dans A, il existe un élément a de A et une partie connexe C de $A \to B$ telle que pour tout $b \in B$, il existe $f \in C$ tel que $f(a) = b$ et $L(f) = a$.*

1.2 Prolongements

Question 4 *Quel est le statut du lemme de l'étoile? Est-il strictement plus faible que l'axiome du choix?*

Le lemme de l'étoile a quelque chose de maximal qui est défini précisément dans le lemme suivant:

Lemme 5 *(Axiome du choix supposé). Soient E, F deux ensembles et T une partie de F^E. On suppose que pour toute L qui soit une application de T dans E, il existe $e \in E$ tel que pour tout $y \in F$ il existe $f \in T$ telle que: $[f(e) = y$ et $L(f) = e]$. Alors $T = F^E$.*

Preuve : La preuve de ça est assez courte: soit $g \in F^E \setminus T$ et $L(f) :=$ un élément $x \in E$ tel que $f(x) \neq g(x)$. Soit $e \in E$ un élément donné par l'hypothèse du théorème. Il s'ensuit qu'il devrait exister $f \in T$ telle que $[f(e) = g(e)$ et $L(f) = e]$, ce qui est contradictoire

Le lemme de l'étoile ne parle que du "e" tel que $\forall y \in F \exists f : f(e) = y$ et $L(f) = e$. MAIS, tel qu'il est formulé, nous n'avons semble-t-il aucun contrôle sur la façon dont f choisit les images $f(x)$ des $x \neq e$.

Les deux énoncés qui suivent montrent qu'on peut obtenir un peu plus d'information ou de contraintes concernant *ces $f(x), x \neq$ le e qui compte*

Théorème 6 *(Axiome du choix). On suppose que F est un ordinal (ou ce qui revient au même est muni d'un bon ordre). Soit $L : (E \to F) \to E$. Alors il existe $e \in E$ et une application $y \mapsto f_y$ qui est croissante de F dans $(E \to F, \leq_{all})$ vérifiant $\forall y \in F : L(f_y) = e$ et $f_y(e) = y$ et de plus $\forall (y, z) \in F^2$: si $y \leq z$ alors $f_y \leq_{all} f_z$ où $f \leq_{all} g$ signifie $\forall x \in E : f(x) \leq g(x)$.*

Preuve : On construit par récurrence ordinale la séquence $g_a, a \in Ordinaux$ de la manière suivante: $g_a(x) :=$ le premier élément y de F tel que $\forall b \in a$ si $L(g_b) = x$ alors $g_b(x) \neq y$. On s'arrête quand g_a ne peut pas être définie. Soit donc le premier ordinal μ tel que g_μ ne puisse pas être définie: il existe alors $x \in E$ tel que $\forall y \in F \exists b \in \mu : L(g_b) = x$ et $g_b(x) = y$. A chacun de ces $y \in F$ on associe $b(y)$ le plus petit possible ainsi, ce qui donne $y \mapsto f_y := g_{b(y)}$ qui vérifie ce qu'on cherche.

Le théorème suivant répond à la question du statut du lemme de l'étoile :

Théorème 7 *dans **ZF** il y a équivalence entre lemme de l'étoile et axiome du choix*

Preuve : Soit A un ensemble. On va démontrer que A peut être muni d'un bon ordre en le mettant en bijection avec un ordinal. On pose $E := P(A)$ et $F := A$. A chaque application $f \in E \to F$ on associe l'élément $L(f) \in E$ suivant: on construit u_f dont le domaine est un ordinal $\mu(f)$ par récurrence ordinale de la manière suivante: $u_f(\alpha) := f(\{u_f(\beta) | \beta \in \alpha\})$ et $\mu(f)$ est le premier ordinal i tel que $u_f(i) \in \{u_f(j) | j \in i\}$. On pose $L(f) := \{u_f(i) | i \in \mu(f)\}$. Par définition, $f(L(f)) \in L(f)$ et $L(f)$ est bien ordonné car u_f est une bijection entre $L(f)$ et un ordinal. Soit $B \in E$, c'est à dire $B \subseteq A$, tel que $\forall y \in F \exists f \in E \to F : L(f) = B$ et $f(B) = y$. On a donc $A = B$ (sinon il y aurait un y et une f telle que $f(B) \notin B$ et $L(f) = B$). Conclusion: A est en bijection avec un ordinal et est donc bien ordonnable.

1.3 Conclusion

Des questions diverses se posent quant à la généralisation possible de ce phénomène émergent équivalent à l'axiome du choix et très proche de la détermination des jeux. Nous ne pouvons pas en donner de liste. Le théorème précédent, où l'ensemble d'arrivée est un ordinal, montre que la famille des f_y telles que pour tout $y : f_y(a) = y$ et $L(f_y) = a$ peut être trouvée ayant "de bonnes propriétés". Ce genre de questions est complexe et dépend des structures de l'ensemble d'arrivée.

Voici un exemple, parmi d'autres, de question intéressante:

Question 8 *Soit* $L :\in (E \to \mathbb{R}) \to E$. *On munit* $\mathbb{R}$ *de sa topologie* T *usuelle et* $E \to \mathbb{R}$ *de la topologie* T_∞ *de la norme sup. Existe-t-il alors forcément* $a \in E$ *et* $\phi : x \mapsto f_x$ *tels que pour tout* $x \in \mathbb{R} : f_x(a) = x$ *et* $L(f_x) = a$ *et de plus* ϕ *continue de* $(\mathbb{R}, T)$ *vers* $((E \to \mathbb{R}), T_\infty)$*?*

La réponse est "non" sinon, la vie serait "trop belle" en quelque sorte, entre autre parce que nous n'avons rien supposé sur L. Mais on n'est pas très loin d'avoir un "oui" partiel sous la forme d'une série de lemmes qui sont généralement classés dans la catégorie des théorèmes de Brouwer

1.4 En l'absence de l'axiome du choix

Avant d'être un axiome de ZFC, l'axiome du choix émerge lors d'implémentations syntaxiques dans les démonstrateurs automatiques en créant des témoins. Même sans formaliser les mathématiques, on ne peut pas exclure des difficultés quand les ensembles sont infinis. De manière évidente (comme le montrent les démonstrations ci-dessus), les preuves telles que celle du détermination des jeux, du lemme de l'étoile, ne sont pas "algébriques". Que peut-il rester d'algébrique des arguments qui permettent d'établir "de la détermination" ou "de l'étoilage"? Nous avons fait quelques recherches sur les questions de détermination algébrique des jeux, mais ils ne rentrent pas dans le cadre de ce travail. Nous en parlerons ultérieurement. La vraie séparation se fait surtout entre les mathématique intuitionnistes et les mathématiques classiques.

Remarque importante : L'axiome du choix est "un axiome constructif" en un certain sens. En effet, **comme tous les autres axiomes de ZF à l'exception de celui d'extensionnalité** il peut prendre la forme $\exists a \forall x (R(x) \iff x \in a)$. En effet :

Théorème 9 *E est bien ordonnable si et seulement si la collection des ordinaux* α *tels qu'il n'y a pas de surjection de* α *sur* E *est un ensemble*

Preuve : C'est évident.

1.5 La réduction ludique, définitions

1.5.1 La définition naturelle

Les degrés ludiques quotientent toutes les situations possibles par une sorte de relation de "simulabilité", en considérant que "l'atome" d'action du joueur est de:

- Recevoir un coup
- En rendre un **en fonction** du coup reçu
- Le reste de sa vie de joueur devant être considérée comme la vie de **d'autres joueurs** dont éventuellement, l'équipe entière, peut avoir l'illusion de *n'être qu'un avec le joueur lui-même*

Pour des raisons de simplicité, ce n'est pas tout à fait l'atome que nous avons retenu. En effet, le joueur a connaissance, au moment où il rend son coup, pas seulement du coup reçu, mais aussi de "sa position géographique" ou plutôt de son numéro de joueur. Nous n'avons pas développé la position du joueur qui ignore "son numéro de maillot" en quelque sorte, mais elle aurait un sens. Voici les définitions:

Définition 10 *Soit I un ensemble et $i \in I \mapsto (E_i, F_i)$ une famille de couples d'ensembles. Soit $i \in I \mapsto (E'_i, F'_i)$ une famille de couples d'ensembles. Soit $G; H$ respectivement inclus dans $T_1 := \prod_i (E_i \times F_i); T_2 := \prod_i (E'_i \times F'_i)$.*

On dira que $(T_1, g) \leq_{ludique} (T_2, H)$ quand il existe $i \mapsto (f_i \in (E_i \to E'_i), g_i \in ((E_i \times F'_i) \to F_i))$ telle que pour tout $x \in \prod_i E_i$, pour tout $y' \in \prod_i F'_i$: si $[i \mapsto (f_i(x_i), y'_i)] \in H$ alors $[i \mapsto (x_i, g_i(x_i, y'_i))] \in G$

On appelle le préordre $\leq_{ludique}$ la *réduction ludique* et les classes d'équivalence canoniques obtenues s'appellent des *degrés ludiques*

On remarque que chaque ensemble "d'indices" donne un préordre séparé des autres. Son cardinal sera appelé selon les sections l'arité ou encore l'uplicité. En réalité, ce qu'il faudrait appeler arité ou uplicité c'est I lui-même. Dans la plupart des cas nous nous occuperons de situations où I est fini. De plus quand I et J sont en bijection, on peut en un certain sens comparer les I degrés et les J degrés mais cela parait un peu artificiel.

1.5.2 Définitions plus commodes à écrire

L'isomorphisme naturel qui envoie $i \mapsto (x_i, y_i)$ sur $([i \mapsto x_i], [i \mapsto y_i])$ nous conduira aussi à définir la réduction ludique de cette autre manière:

Définition 11 *On appelle "garantie téléphonique d'uplicité n" ou "garantie" (tout court, si aucune confusion n'est possible) un triplet de la forme: (E, S, G) tel qu'il existe des ensembles E_i, S_i pour chaque $i \in n$ avec:*

- *E est le produit des $E_i, i \in n$ et*
- *S est le produit des $S_i, i \in n$ et*
- *G est inclus dans $E \times S$*

Cette définition plus commode dans certains contextes est beaucoup plus artificielle car elle passe trop sous silence l'essence insécables des paires (E_i, F_i) qu'on appellera combinés. Dans son contexte, la définition de la réduction ludique peut se faire en enchainant comme suit les trois définitions suivantes, les deux premières ne servant plus dans la suite:

Définition 12 *Soit E un produit d'ensembles $E_i, i \in I$ et f une fonction dont le domaine est E. On dit qu'elle est* **locale** *sur E quand il existe une famille de fonction h_i de domaines E_i telle que pour tout $x \in E$, pour tout $i \in I : f(x)(i) = h_i(x_i)$*

Définition 13 *Soit E, F deux produits d'ensembles respectivement $E_i, F_i; i \in I$ et f une fonction dont le domaine est $E \times F$. On dit qu'elle est* **bilocale** *sur $E \times F$ quand il existe une famille de fonction h_i de domaines $E_i \times F_i$ telle que pour tout $(x; y) \in E \times F$, pour tout $i \in I : f(x, y)(i) = h_i(x_i, y_i)$*

Définition 14 *Soit n un entier naturel. Soient R, S deux garanties d'uplicité n.*

On dit que R est **ludiquement inférieure ou égale** *à S et c'est noté $R \leq_{lud}$ quand il existe un couple (f, g) avec f locale sur $Entre_R$ et g bilocale sur $Entree_R \times Sorties_S$ vérifiant: pour tout $x \in Entree_R$ et tout $y \in Sorties_S$: si $(f(x), y) \in S$ alors $(x, g(x, y)) \in R$*

Nous avons signalé cette concurrence de deux définitions (non équivalentes, même si isomorphes) car il semble difficile de faire un choix arbitraire. La première est la plus *fondatrice* dans le sens qu'elle respecte bien l'aspect téléphonique des objets abstraits qui sont concernés.

Avant de continuer l'étude des degrés ludiques, remarquons un cas particulier important qui a beaucoup été étudié: *les degrés de Tukey*. On utilise la première définition ci-dessus.

On s'intéresse aux téléphones à deux combinés (indicés par $2 := \{0; 1\}$), mais qui de plus ont la propriété suivante: l'écran du combiné1 est de cardinal 1. Le clavier du combiné2 est de cardinal 1. **Dans ces conditions, l'utilisateur du combiné1 est obligé de se concevoir comme un émetteur et l'utilisateur du combiné2 est obligé de se concevoir comme un récepteur**. Rappel: $1 := \{0\}$

On est face à des téléphones dont la garantie, qui au départ est un ensemble de quadruplets inclus dans $(E \times 1) \times (1 \times F)$, peut se concevoir comme une partie de $E \times F$ et on a le théorème évident suivant:

Théorème 15 *Soient $a := ((E \times 1) \times (1 \times F), G)$ et $b := ((E' \times 1) \times (1 \times F'), G')$ deux garanties ludiques d'uplicité 2. Alors $a \leq_{ludique} b$ si et seulement s'il existe $f \in (E \to E')$ et $g \in (F' \to F)$ telle que pour tous $x \in E$, tout $y \in F'$ si $([f(x), 0], [0, y]) \in G'$ alors $([x, 0], [0, g(y)]) \in G$*

On obtient exactement la notion connue sous le nom de *réduction de Tukey*. Nous consacrons l'un des chapitres suivants à rappeler des résultats de base sur les degrés de Tukey. Avant, nous consacrons un chapitre analogue pour la réduction ludique, où nous utiliserons systématiquement la définition 14 produite ci-dessus.

Chapitre 2

Lemmes de bases sur les degrés ludiques

2.1 Définitions de base, problèmes de notation

Les notions ensemblistes permettent une formalisation parfaite à partir de trois signes: $\forall; \in; \rightarrow$. Cependant, on a deux notions de produits qui sont rappelées ci-dessous, parmi d'autres rappels.

- Le couple (a, b) est l'ensemble $\{\{a\}; \{a, b\}\}$
- Une relation binaire R (c'est à dire un ensemble de couples) est dite fonctionnelle (on dit que c'est une fonction) quand pour tous x, y, z si $(x, y) \in R$ et $(x, z) \in R$ alors $y = z$
- Le domaine d'une fonction f est la première projection, ie l'ensemble des x tels qu'il existe y tel que $(x, y) \in f$.
- Dans la suite on aura très souvent besoin de la notion de produit. Soit f une fonction de domaine D. On peut la regarder comme une famille d'ensembles, et dans ce cas, on note souvent $(f_i, i \in D)$ à la place de f. Le produit de f est l'ensemble des fonctions g telles que:
- dom(g)=D et pour tout $i \in D : g(i) \in f(i)$
- On rappelle que quand $n \in \mathbb{N}$, l'entier naturel n est l'ensemble des entiers naturels qui lui sont strictement inférieurs.
- Il pourra parfois y avoir des ambiguités quand $dom(f) = 2$.
- En effet, le produit de f est alors très ressemblant (pour le lecteur) à $f(0) \times f(1)$.
- Pour bien l'en distinguer, je noterai souvent $[f(0) \times f(1)]$ à la place de $f(0) \times f(1)$ pour désigner le produit de f.
- Par contre, d'une manière systématique, j'utiliserai aussi bien $x(y)$ que x_y sans que ces deux notations ne désignent des objets différents.

2.2 Avertissement

Du fait qu'on va devoir à plusieurs endroits opérer des permutations de combinés ou jouer sur plusieurs tables, nous avons choisi, comme annoncé en introduction, d'adopter un point de vue *triplet (E:=produit des Entrées, F:=produit des Sorties, Garantie incluse dans $E \times F$).* C'est hélas un peu contraire au principe même que nous avons défendu en introduction, mais plus commode. En effet, 'l'objet matériel" est le combiné téléphonique. La présentation en triplet pourrait induire vers l'erreur à ne même plus appliquer le même ensemble d'indices pour les entrées et les sorties, autrement dit, les claviers et les écrans. Espérons que cet avertissement suffise à lever toute ambiguité. **Nous répétons donc les définitions choisies.**

2.3 Définitions et théorèmes de base sur les degrés ludiques

Définition 16 *On appelle "garantie téléphonique d'uplicité n" ou "garantie" (tout court, si aucune confusion n'est possible) un triplet de la forme: (E, S, G) tel qu'il existe des ensembles E_i, S_i pour chaque $i \in n$ avec:*

- *E est le produit des $E_i, i \in n$ et*
- *S est le produit des $S_i, i \in n$ et*
- *G est inclus dans $E \times S$*

Par abus de langage on nomme aussi parfois G le triplet (E,S,G), et on se réfère parfois à E et S en les notant respectivement $Entree(G), Sortie(G)$

La plupart du temps, n sera un entier naturel > 1, mais la définition supporte parfaitement que ce soit **un ensemble quelconque**.

Le GHZ-téléphone est d'uplicité 3. Certains téléphones quantiques importants sont d'uplicité 2. Concrêtement, l'entier n est le nombre de combinés du "téléphone", et ses élément sont les numéros des combinés.

E_i est l'ensemble des touches du clavier du combiné numéro i et S_i est l'ensemble des sorties possibles sur l'écran du combiné i. L'ensemble G est **la garantie**

Nous avons défini dans le chapitre précédent les notions de "fonction locale" et "fonction bilocale" (voir les définitions 12 et 13). Nous rappelons ci-dessous la notion de réduction ludique déjà donnée dans le même chapitre :

Définition 17 *Soit n un entier naturel. Soient R, S deux garanties d'uplicité n.*

On dit que R est **ludiquement inférieure ou égale** *à S et c'est noté $R \leq_{lud} S$ quand il existe un couple (f, g) avec f locale sur $Entre_R$ et g bilocale sur $Entree_R \times Sortie_S$ vérifiant: pour tout $x \in Entree_R$ et tout $y \in Sortie_S$: si $(f(x), y) \in S$ alors $(x, g(x, y)) \in R$*

Lemme 18 *: $\leq_{lud}$ est transitive*

Preuve : Soient f, g locale (resp bilocale) qui témoignent que $R \leq S$ et k, h locale (resp bilocale) qui témoignent que $S \leq T$. Soit $u : x \in Entree_R \mapsto k(f(x) \in Entree_T$ et $v : (x, z) \in Entree_R) \times Sortie_T \mapsto h(f(x), g(x, k(x, z)))$ Les fonctions u, v sont alors respectivement locales, bilocales et réduisent R à T

La relation $\leq_{lud}$ est donc une relation de préordre sur la classe des garanties téléphoniques ayant la même uplicité. Elle induit comme il est usuel une relation d'ordre et une relation d'équivalence de telle sorte qu'en passant au quotient, les classes d'équivalence soient ordonnées.

Par abus de langage, s'il n'y a pas d'ambiguité, on abrègera souvent $\leq_{lud}$ en écrivant $\leq$. Le contexte est censé rendre clair le sens des différentes occurrences de $\leq$ dans le texte.

Définition 19 *Deux garanties téléphoniques R, S sont dites (ludiquement) équivalentes quand $R \leq S$ et $S \leq R$. Lorsqu'elles sont équivalentes on dit qu'elles ont le même degré ludique et réciproquement. Ainsi les degrés ludiques sont les classes d'équivalence modulo la relation d'équivalence: X, Y* **sont (ludiquement) équivalentes**

Soit n un ensemble et (E, F, R) une garantie téléphonique d'uplicité n.

Définition 20 *Elle est dite triviale quand il existe une application locale de E dans F incluse (dont le graphe est inclus) dans R.*

Il arrivera parfois, pour alléger l'aspect cabalistique du texte qu'on confonde un téléphone (qui n'est pas défini mathématiquement dans ce texte) et sa garantie.

2.3.1 Commodités, abus de langage

Comme cela se passe avec les degrés de Tukey (que nous verrons dans le chapitre suivant), il y a des opérations auxquelles la notion de degré ludique est insensible.

Par exemple, on peut toujours supposer que la garantie d'uplicité n dont on cherche à analyser le degré ludique est de la forme (E, E, R) avec $R \subseteq E^n \times E^n$, ceci étant valable quelque soit **l'ensemble** n.

Théorème 21 *Soit $(E := \prod_i E_i, F := \prod_i F_i, R)$ une garantie ludique, le produit étant pris sur un ensemble n quelconque. Alors il existe un triplet (U, U, S) tel que $(E, F, R) ==_{ludique} (U, U, S)$*

Preuve : Soit U un ensemble tel que $\forall i \in n : E_i \cup F_i \subseteq U$. Soit S l'ensemble des couples $(x, y) \in (U^n)^2$ tels que si $x \in \prod_i E_i$ alors $(y \in \prod_i F_i$ et $(x, y) \in R)$. Alors (U, U, S) convient

2.4 Degrés maximaux et minimaux

Théorème 22 *: pour toute uplicité, il existe un degré minimum et un degré maximum. Deux garanties téléphoniques triviale de même uplicité sont ludiquement équivalentes et ludiquement inférieures à toute autre.*

- Le degré maximum pour l'uplicité n est celui, par exemple, de $(1^n, 1^n, \emptyset)$

- Le degré minimum est celui de n'importe quelle garantie téléphonique triviale, comme par exemple $\mathbb{N}^n, \mathbb{N}^n, \mathbb{N}^n \times \mathbb{N}^n$

  Preuve : C'est évident

Définition 23 *Comme pour les degrés de Tukey et quand ça ne génèrera pas d'ambiguité, on appellera* $TopLudique_n$ *et* $BottomLudique_n$ *les degrés maximums resp minimums d'uplicité* n*. On omettra éventuellement l'indice* n*. Il arrivera aussi qu'on appelle par le même nom un représentant et son degré.*

Les sections suivantes montrent qu'on a des degrés formant des classes cofinales canoniques, ie des degrés presque minimaux ou presque maximaux:

2.5 Opération duale

Soit (E, F, G) une garantie d'uplicité n tel que E est le produit (ensembliste) des ensembles $E_i, i \in n$ et F est le produit des ensembles $F_i, i \in n$.

Soit $E'_i := F_i^{E_i}$ l'ensemble des applications de E_i dans F_i. Notons E' le produit des $E'_i, i \in n$. Etant donné $x \in E'$ et $y \in E$, on note $x * y$ l'application de n dans F (i.e; l'élément de F) qui à chaque $i \in n$ associe $x(i)(y(i))$

Soit H l'ensemble des couples $(x, y) \in E' \times E$ tels que $(y, x * y) \notin G$

Définition 24 *Le triplet* (E', E, H) *est appelé le dual de* (E, F, G)*. On appelle biduale d'une garantie la duale de sa duale.*

Le théorème suivant et ceux qui suivent signalent que l'opération duale joue pour les degrés ludiques le même rôle que l'opération duale des degrés de Tukey.

Théorème 25 *Une garantie et sa biduale ont le même degré ludique*

Il y a un sens presque évident et l'autre qui utilise l'axiome du choix dans le cas le plus général. A noter que si tout est fini (l'uplicité, l'entrée, la sortie) l'axiome du choix n'est pas nécessaire. Nous exploitons le lemme de l'étoile que nous rappelons:

Lemme 26 *Soient* E, F *deux ensembles. Soit* L *une application de* F^E *dans* E*. Alors il existe* $e \in E$ *tel que pour tout* $y \in F$ *il existe* $f \in F^E$ *telle que:* $f(e) = y$ *et* $L(f) = e$*.*

> Preuve : Pour des raisons de commodité d'écriture, on omet de préciser les domaines des fonctions considérés. Cela donne une écriture dans le genre suivant: *un couple* (f, x) *est un élément de la duale de* R *quand* $(x, f * x)$ *n'appartient pas à* R *un couple* (L, f) *est un élément de la biduale de* R *quand:* $(f, L * f)$ *n'est pas dans la duale de la duale de* R*, autrement dit quand:* $(L * f, f * (L * f))$ *est un élément de* R Le sens le plus facile est de prouver que la biduale T de R est $\geq R$. En effet, à chaque x_i tapé sur le clavier du combiné i que l'on veut mimer, on tape la fonction constante $L_i : f \mapsto x_i$ sur la clavier i du téléphone T-garanti. L'écran i renvoie alors une réponse $f_i \in Sortie_T$ de sorte que $([i \mapsto L_i(f_i)], [i \mapsto f_i(L_i(f_i))]) \in R$; donc $([i \mapsto x_i], [i \mapsto f_i(x_i)]) \in R$ et donc on peut renvoyer en sortie sur chaque combiné i, la réponse $y_i := f_i(x_i)$ de sorte qu'on aura réussi en procédant localement à mimer un R-téléphone (en effet $(x, y) \in R$) L'autre sens utilise le lemme de l'étoile. On souhaite mimer un T-téléphone en utilisant un R-téléphone. L'utilisateur tape donc L_i sur le combiné i. D'après le lemme de l'étoile, il existe $e_i \in E_i$ tel que pour toute $y \in F_i$, il

existe $f \in F_i^{E_i}$ avec $f(x_i) = y$ et $L_i(f) = e_i$. On tape e_i sur le R-téléphone dont on dispose et on reçoit $r_i \in F_i$ tel que $(i \mapsto e_i, i \mapsto r_i) \in R$ Or il existe f_i telle que $L_i(f_i) = e_i$ et $f_i(e_i) = r_i$. On peut donc renvoyer en sortie sur le combiné i, la réponse f_i avec la garantie que $(i \mapsto L_i, i \mapsto f_i) \in T$.

Théorème 27 *Sur la classe des degrés ludiques d'uplicité n, l'opération $d \mapsto dual(d)$ est un isomorphisme involutif de $(Degres, \leq)$ sur $(Degres, \geq)$*

Preuve : Il reste à justifier que $R \leq S \Rightarrow dual(S) \leq dual(R)$. On suppose donc qu'il existe une réduction de R à S que l'on schématise comme suit: $x_i \to s_i(x_i) \mid y_i \to k_i(x_i, y_i)$. Voici le schéma de la réduction en chaque combiné i:

$$f_i \to x \mapsto k_i(x_i, f_i(s_i(x))) \mid q_i \to s_i(q_i)$$

2.6 bornes inférieures, supérieures

On commence par prouver l'existence de la borne supérieure, puis la borne inférieure s'en déduit par dualité. Soit une famille de garanties téléphoniques $R_i, i \in J$ qui sont toutes de même uplicité n. Remarque: n peut être n'importe quel ensemble ici.

Théorème 28 *Il existe une garantie téléphonique S, d'uplicité n, telle que: Pour tout $i \in J : R_i \leq S$ et toute garantie téléphonique Z d'uplicité n telle que $\forall i \in J : R_i \leq Z$ vérifie $S \leq Z$*

Autrement dit: toute famille (indicée par un ensemble) de degrés ludiques a une borne supérieure.

Preuve : Voici la définition d'une S qui convient:

- pour $p \in n : Entree_S(p) :=$ la réunion quand i parcourt J des $Entree_{R_i}(p) \times J$
- pour $p \in n : Sortie_S(p) :=$ la réunion quand i parcourt J des $Sortie_{R_i}$

On note E' le produit des $Entree_S(p), p \in n$ et $S' :=$ le produit des $Sortie_S(p), p \in n$. De même, pour $x \in Entree_S$, chaque $x(p)$ est de la forme $(u(p), j(p))$ et u sera alors noté par $proj1(x)$. $G_S :=$ l'ensembles des couples $(x, y) \in E' \times S'$ tels que: si $\forall (p, q) \in n^2 : p = q (=: e)$ alors $(proj1(x), y) \in R_e$. Alors $S := (E', S', G)$ vérifie l'affirmation du théorème. La borne inférieure vient ensuite par dualité, nous écrivons donc le théorème suivant sans preuve.

Théorème 29 *: toute famille de degrés ludiques indicée par un ensemble a une borne inférieure*

2.7 Degrés presque minimaux et presque maximaux

L'opération duale a une utilité immédiate qui est de "trouver" sans inspiration des degrés gros quand on en connait des petits et réciproquement. Soient E un ensemble, n un entier et F l'ensemble E^n. Soit G l'ensemble des $(x, y) \in E^n \times F^n$ tels que $\forall i \in n : y(i) = x$

A l'évidence cette relation a un degré ludique "presque maximal". Il faut l'entendre dans le sens suivant:

Théorème 30 *La seule garantie téléphonique de la forme (E^n, F^n, H) qui ne soit pas ludiquement réductible à (E^n, F^n, G) a le degré TopLudique*

Preuve : Soit en effet $H \subseteq E^n \times F^n$ tel que $\forall x \in E^n \exists y \in F^n : (x, y) \in H$. Il est très facile de mimer un H-téléphone en se servant d'un G-téléphone. En effet, tapant x_i sur le clavier i, on reçoit x sur tous les écrans. Il suffit à partir de ce x, de choisir y tel que $(x, y) \in H$ et de renvoyer y_i sur l'écran du combiné i

La dualité permet alors de dire que la duale de (E^n, F^n, G) est en quelque sorte "presque minimale". Cette dualité donne un guide pour décrire les degrés juste au dessus des non triviaux. D'une manière générale, on les appellera informellement des degrés *Anticantor*. Explicitons ce que c'est dans le cas particulier de l'uplicité 2:

Soit (E^2, F^2, R) une garantie téléphonique non triviale. On sait donc que pour tout couple d'applications f_1, f_2 de E_i dans F_i il existe $(x_1, x_2) \in E^2$ tel que $((x_1, x_2), (f_1(x_1), f_2(x_2))) \notin R$. Par le lemme de l'étoile, l'alternance des quantificateurs de l'énoncé précédent donne:

$$\forall f_1 \; \forall f_2 \; \exists x_2 \; \exists x_1 \; [...]$$

donc

$$\forall f_1 \; \exists x_2 \; \forall r_2 \; \exists f_2 \; \exists x_1 \; [...] \;\; et \;\; r_2 = f_2(x_2),$$

qui montre que voyant f_1, on peut jouer un certain x_2 tel que pour tout y_1, r_1, r_2 si $([y_1, r_1], [x_2, r_2]) \in R$ alors $x_1 \neq y_1$ ou $r_1 \neq f_1(x_1)$. Or cette assertion est exactement la démonstration qu'on peut mimer un U-téléphone avec un R-téléphone en définissant la garantie du U-téléphone par $([Entre1 \times Entre2], [Sortie1 \times Sortie2], U)$:

- Entrée1 $:= E_1 \to F_1$ Entrée2 $:= E_1$ Sortie1 $:= E_1$ Sortie2 $:= F_1$
- $U :=$ l'ensemble des $([f_1, x_1], [u, v])$ tels que si $x_1 = u$ alors $f_1(x_1) \neq v$
- La stratégie de mimage étant:

$$y_1 \to y_1 \mid r_1 \to r_1$$

$$f_1 \to x_2 \mid r_2 \to x_1$$

Nous avons ainsi démontré le théorème suivant:

Théorème 31 *La garantie U précédente est $\leq$ à n'importe quelle garantie non triviale de la forme $([E_1 \times E_2], [F_1 \times F_2], R)$*

Nous pouvons proposer une notation précise:

Définition 32 *la garantie U précédente (qui ne dépend que de E_1, F_1) sera notée $Anticantor(E_1, F_1)$*

2.8 Classes importantes de degrés ludiques

2.8.1 Uplicité 2

Dans cette section, nous introduisons la motivation générale qui a conduit à cette étude de "téléphones" dans le cadre simplifié de l'uplicité2. L'un des premiers points importants dans le paradoxe EPR est l'impossibilité d'utiliser un téléphone quantique pour transmettre un message causal. Encore faut-il définir formellement ce qu'est un message. La réponse est assez simple ou plus précisément **est rendue assez simple** par la considération des degrés de Tukey, qui formalisent la notion de “quantité d'information” unitaire.

Définition 33 *Soit $v := (E, F, R)$ une relation de Tukey et $e := (A, B, S)$ une relation ludique d'uplicité 2. On dira que e permet d'envoyer un v-message de 0 vers 1 quand $pl(v) \leq_{ludique} e$ (pl est définie formellement dans le chapitre qui détaille l'étude des degrés de Tukey)*

Le fait de ne pas pouvoir se servir d'un téléphone ludique pour envoyer un v-message doit bien entendu ne pas dépendre du combiné par lequel on a choisi d'émettre.

Définition 34 *On dit que e ne permet pas d'envoyer un v-message quand il ne le permet ni de 0 vers 1, ni de 1 vers 0.*

Cela nécessite donc de prendre en considération les garanties obtenues à partir de e en permutant les combinés. De manière générale, on a donc besoin de la définition suivante:

Définition 35 *Soit $e := (E := \prod_i E'(i), F := \prod_i F'(i), S)$ une relation ludique d'uplicité n (la lettre n ne désigne pas forcément un entier). Soit s une permutation de n. On note $permut(e, s)$ la relation ludique (A, B, G) obtenue de la manière suivante: $A'(i) := E'(s(i))$ et $B'(i) := F'(s(i))$ et $A := \prod_i A'(i)$ et $B := \prod_i B'(i)$ et $G :=$ l'ensemble des couples $(x, y) \in A \times B$ tels que $(x \circ s^{-1}, y \circ s^{-1}) \in S$*

Remarque : Si $x \in A$ alors $x \in \prod_i A'(i) = \prod_i E(s(i))$, donc $\forall i \in n : x(i) \in E(s(i))$ donc $\forall i \in n : x \circ s^{-1}(i) \in E'(i)$ donc $x \circ s^{-1} \in \prod_i E'_i = E$

Cette description est abstraite mais en pratique, les choses sont simples quand n est petit. La garantie $permut(e, s)$ est simplement attachée à un téléphone e-garanti T dont on utiliserait les combinés dans un "ordre" différent, précisément le combiné i du nouveau téléphone devenant le combiné numéro $s(i)$ de T

2.9 Degrés TSD

Une relation ludique d'uplicité2 est TSD quand elle permet de transmettre *au moins un tout petit peu d'information*. Que signifie ce "au moins un petit peu"? La réponse est naturelle: l'émetteur envoie $x \in E$ et le récepteur reçoit un $y \neq x$ tel que $y \in E$. Evidemment cette notion n'a un sens que relativisée à un ensemble E (et en présence de l'axiome du choix, simplement son cardinal). Autrement dit, on s'intéresse aux degrés de Tukey les plus petits possibles qui ne soient pas simplement le degré de Tukey $UnTukey$ (qui ne transmet strictement rien et est simulable par un téléphone en plastique pour enfants des années 1950). Cela donne la définition suivante.

Définition 36 *Soit $w := (E, F, R)$ une relation ludique où E est de la forme $[E_0 \times E_1]$ et F est de la forme $[F_0 \times F_1]$. On dit qu'il est nonTSD quand:*

$$\forall x_0 \in E_0 \exists y_0 \in F_0 \forall x_1 \in E_1 \forall y_1 \in F_1 : (x, y) \in R$$

et

$$\forall x_1 \in E_1 \exists y_1 \in F_1 \forall x_0 \in E_0 \forall y_0 \in F_0 : (x, y) \in R$$

. quand une relation ludique n'est pas non TSD on dit qu'elle est TSD.

Autrement dit, w est non TSD quand on ne peut pas utiliser un w-téléphone ludique pour envoyer un message d'un combiné vers l'autre.

2.10 Généralisation à l'uplicité finie

On rappelle qu'il y a dans chaque degré ludique un représentant de la forme (E, E, G) (que l'on note aussi parfois G par abus de langage). Dans ce cas l'usage des quantificateurs, quand il n'y a pas d'ambiguïté possible, est entendu restreint à E ou plus élégamment, on considère que quand $x \notin E^n$ alors n'importe quel r respecte la garantie.

Définition 37 *Soit n un entier et G une garantie ludique adéquate. On note S_n l'ensemble des permutations de n. La garantie G est dite nonTSD si:*

$$\forall s \in S_n : \forall x_0 \exists r_0 \forall x_1 \exists r_1 ... \forall x_{n-1} \exists r_{n-1} : (x \circ s, r \circ s) \in G$$

Cette définition exprime que quelque soit l'ordre **temporel** dans lequel sont placés les utilisateurs de combinés, ils ne pourront pas "prouver" de manière indiscutable que les combinés leur permette d'envoyer de l'information.

2.11 Degrés MULTITABLE

Quand on joue sur plusieurs tables en essayant de gagner sur au moins une, on s'en trouve dans une situation facilitée, d'autant plus facilitée que le nombre de tables est grand par rapport à une situation où la table où on doit gagner est imposée.

Un téléphone multitable est, pour parler intuitivement, un téléphone tel qu'en jouant sur plusieurs tables, on assure sa garantie sur au moins une table SANS COMMUNIQUER avec ses complices qui simulent les autres combinés (sur la même "multitable"). Il est donc évident qu'une garantie multitable NE PEUT PAS permettre aux utilisateurs de téléphones à qui on a promis cette garantie de communiquer entre eux quelque chose de l'ordre d'un "vrai message" causal puisque les simulateurs cachés dans le téléphone parviennent à le faire fonctionner sur au moins une table en ne rompant pourtant jamais la séparation totale qui les isole combiné par combiné et en ayant une action locale, certes multitable, mais complètement concrète. La définition formelle est un peu lourde et pour éviter que les redites, on la définit directement pour une uplicité quelconque.

Soit $e := (E := \prod E_i, F := \prod F_i, R)$ une garantie ludique d'uplicité n. Soit c un cardinal. Dans la suite ce cardinal c représente le nombre de tables sur lesquelles on va tenter de simuler le téléphone.

Définition 38 *La garantie e est dite c-multitable quand pour chaque $i \in n$, il existe une application f_i de E_i^c dans F_i^c telle que pour tout $x \in \prod_i (E_i^c)$ si pour tout $(i, z) \in (n, c)$ on note $y(z)(i) := f_i(x(i))(z)$ et $d(z)(i) := x_i(z)$ alors il existe $z \in C$ tel que $(d(z), y(z)) \in R$. Une garantie est dite multitable quand il existe c tel qu'elle soit c-multitable*

Il est évident qu'une garantie multitable est nonTSD. Le théorème suivant affirme la réciproque.

Théorème 39 *Une garantie d'uplicité2 est multitable si et seulement si elle est nonTSD*

La preuve qui suit établit le théorème en supposant l'hypothèse généralisée du continu. Il est possible de se passer de HC au prix de complications techniques de la même façon que le lemme de Ketonen intervient pour éliminer l'hypothèse du continu dans la démonstration que deux multirelations sont logiquement équivalentes si et seulement si elles admettant des ultrapuissances isomorphes.

2.11.1 Résumé de la preuve

La preuve utilise des notations qui sont lourdes. Le résumé permettra au lecteur de se faire une idée globale du principe. Face à l'entrée x sur le combiné0, en jouant sur plusieurs tables, le simulateur est devant un produit de $x := x_z, z \in c$. Il ne peut pas communiquer avec son complice qui voit, lui, le produit $y := y_z, z \in c$.

L'hypothèse du continu (l'axiome du choix étant supposé) permet de trouver un bon ordre sur ces produits tel que si $x \leq y$ alors l'objet x a une numéro qui est dans c, par exemple disons t, **car l'ensemble des x tels que $x \leq y$ s'injecte dans** c.

Cela entraîne que le simulateur du combiné1, celui qui voit y, peut essayer toutes les réponses correctes possibles, en étant ainsi sûr que sur la table t qu'il ne connaît pas, le "quadruplet" $([x_t, y_t], [amnesie_t, essai_t])$ va faire bingo.

C'est à cet endroit-là que l'hypothèse nonTSD est utilisée: en effet, il faut pour cela que le simulateur du combiné0, celui qui ne voit que les x_z ait joué, en ce qui concerne la table t, une réponse en fonction de x_t et seulement en fonction de x_t or c'est précisément ce que permet l'hypothèse $\forall x \exists a \forall y \exists r : ([x, y], [a, r]) \in R$. Bon ça, évidemment c'est quand $x \leq y$.

Mais il faut aussi envisager que $y \leq x$ et dans ce cas, il faut s'être préservé une possibilité d'avoir gardé la moitié des numéros pour inverser les rôles des simulateurs, ce que permet l'hypothèse du continu

2.11.2 Remarque

Le schéma précédent permet d'ailleurs de comprendre qu'essentiellement **la même preuve** conduit au résultat un peu plus général suivant:

Théorème 40 *Une garantie d'uplicité finie est multitable si et seulement si elle est nonTSD*

2.12 Preuve détaillée du théorème nonTSD = multitable

2.12.1 Introduction

Le fait que $Multitable \subseteq nonTSD$ est facile. Pour démontrer l'inclusion inverse, nous admettons, comme nous l'avons dit plus haut, l'hypothèse généralisée du continu.

2.12.2 Réduction à un cas particulier canonique

Soit n un entier. La classe nonTSD des téléphones d'uplicité n admet une sous-classe cofinale dont la définition est pure. On note S_n l'ensemble des permutations de n.

Soit E un ensemble. On note $Gene(n, E)$ la garantie du téléphone à n combinés dont les claviers sont E et les écrans sont E^n, et qui est l'ensemble des $(x, y) \in E^n \times (E^n)^n$ tel que pour tout $i \in n$ et pour tout $j \leq i : y(i)(j) = x(j)$.

On note $genp(n, E)$ le téléphone avec mêmes combinés, mais dont la garantie est

$$\exists s \in S_n : (x \circ s, y \circ s) \in gene(n, E)$$

Lemme 41 *Pour tout ensemble E est tout entier n, et tout téléphone nonTSD T dont claviers et écrans sont inclus dans E, il existe un ensemble F tel que $T \leq_{ludique} genp(n, F)$. En outre, $genp(n, F)$ est nonTSD*

Il s'ensuit que nous pouvons sans perte de généralité prouver le théorème en supposant que le téléphone nonTSD est de la forme $genp(n, E)$.

2.12.3 Hypothèse du continu

La manière dont va être utilisée l'hypothèse du continu est la suivante: une bonne fois pour toute, on a un téléphone $genp(n, E)$ fixé pour toute la suite. On suppose l'existence d'un cardinal κ et d'un bon ordre $<$ sur $F := (E^\kappa)$ tel que pour tout $x \in F$: le cardinal de l'ensemble des y tels que $y \leq x$ est $\leq \kappa$.

On structure l'ensemble des tables. Cet ensemble a le même cardinal que E. On le note T, et il s'agit de $n! \times E^n$.

2.12.4 Fin de la preuve

Les fonctions ϕ^i_G, pour $i \in n$ sont définies par le contexte. Nous n'en donnons pas de définition explicite pour ne pas alourdir davantage la démonstration.

Soient, pour chaque combiné $i \in n$, un uplet $x(i) := t \in T \mapsto x(i)(t)$, qui représente notre mise à l'épreuve sur les T tables pour le combiné numéro i. L'un des $n!$ groupes de tables correspond à une permutation s de S_n telle que $x(s(0)) \leq .. \leq x(s(n-1))$. Sans perte de généralité, on se concentre sur ce groupe G de tables et on y décrit comment on répond aux touches tapées sur les claviers. On suppose donc que $s = id$.

Sur le combiné 0, on se contente de recopier $(z, 0, 0..0)$ sur chaque écran de chaque combiné de chaque table, la touche pressée z au clavier. Autrement dit, on répond $y(0)(x)(t)(0) := x(0)(t)$.

Sur le combiné 1, (i.e. le deuxième combiné du téléphone), pour chaque table t du groupe, on regarde $x' := \phi^1_G(x(1), t_0)$ et on envoie à l'écran de la table t la réponse $(x'(0)(t_0), x(1)(t), 0, 0..)$. Remarquons qu'on connait $x(1)$ puisqu'on est entrain de parler du combiné1.

Sur le combiné 2, ie le troisième combiné du téléphone, pour chaque table t du groupe, on regarde $(x'(0), x'(1)) := \phi^2_G(x(2), t_1)$ et on envoie à l'écran de la table t la réponse $(x'(0)(t), x'(1)(t), x(2)(t), 0, .., 0)$

Et ainsi de suite...

Il reste à justifier qu'il existe **au moins une table** $(t_0, .., t_{n-1})$ telle que la garantie du téléphone a été réalisée. Il existe t_{n-1} tel que en posant $(y_0, .., y_{n-2}) := \phi_G^{n-1}(x(n-1))$ on a eu raison de penser face au combiné $n-1$, alors qu'on ne le sait pas à priori, que $(y_0, .., y_{n-2}) = (x_0, .., x_{n-2})$, ceci étant dû au fait que tous les x_i sont $\leq x_{n-1}$.

De la même façon, il existe t_{n-j} tel que en posant $(y_0, .., y_{n-j}) := \phi_G^{n-j}(x(n-j+1))$ on a eu raison de penser face au combiné $n-j$, alors qu'on ne le sait pas à priori, que $(y_0, .., y_{n-j}) = (x_0, .., x_{n-j})$, ceci étant dû au fait que tous les x_i sont $\leq x_{n-j}$ quand $i < n-j+1$. Finalement, la table $t := (t_0, .., t_{n-1})$ présente une garantie réalisée

2.12.5 Conséquence philosophique

Ce théorème montre que la construction par n'importe quelle physique, même hypothétique, d'un téléphone nonTSD ne suffit pas à invalider dans un sens fort l'existence d'au moins une interprétation "localisante", à la condition toutefois de ne pas rajouter dans les postulats un caractère *unimonde* à l'univers. En résumé: en présence du déterminisme (voir ci-dessous) une physique ne peut prétendre fabriquer de téléphones non triviaux. En son absence, la physique peut aller jusqu'à postuler tous les téléphones nonTSD comme constructibles. En revanche, le chapitre 7 montre que si ladite physique souhaite non pas postuler le déterminisme, mais postuler un déterminisme probabiliste, alors la limite se situe au niveau **casino-inoffensif**. La théorie quantique est bien en dessous, comme on le verra dans chapitre 7.

2.13 Degrés issus de la volonté de *mesurer de la magie*

2.13.1 Introduction et précisions

Cette sous-section fait suite au chapitre *paradigme téléphonique* et le complète. La MQ nous confronte à des *prodiges* étonnants, dont l'essentiel du texte en traite finalement principalement UN précis qui est ce qui est connu sous le nom de paradoxe EPR.

Cependant nul besoin de se référer à la physique pour éprouver divers besoins de **mesurer** des niveaux de magie. Voici une liste très naive de questions n'ayant pour l'heure pas de sens mathématique que tout un chacun peut ou s'est peut-être déjà posées.

- à supposer qu'on dispose d'un bureau dans lequel on puisse ranger 8 boules dans 7 tiroirs sans mettre plus d'une boule par tiroir: peut-on moyennant quelques opérations de menuisier en tirer un bureau dans lequel on puisse ranger 8 boules dans 7 tiroirs sans mettre plus d'une boule par tiroir?
- à supposer qu'on dispose d'un bureau dans lequel on puisse ranger 8 boules dans 7 tiroirs sans mettre plus d'une boule par tiroir: peut-on moyennant quelques opérations de menuisier en tirer un bureau dans lequel on puisse ranger 9 boules dans 8 tiroirs sans mettre plus d'une boule par tiroir?
- à supposer qu'on puisse sortir d'un cercle sans lever le stylo, peut-on sortir du rectangle sans lever le stylo?
- à supposer qu'on dispose d'une application continue de $[0; 1]$ dans lui-même sans point fixe, peut-on construire en l'utilisant une file de pièces de couleur unie, telle que la première soit verte, la dernière soit rouge, et que deux pièces consécutives soient de même couleur?

- Quel est le niveau de magie apporté une surjection de E sur $P(E)$? Permet-il à supposer qu'on puisse y accéder de construire l'un des objets impossibles précédents?
- Quels sont les niveaux de magie apportés par le fait de disposer de **téléphones quantiques**? Permettent-ils de transmettre de l'information instantanément? Mais ce n'est pas la seule question (même si c'est la seule qui a été traitée jusqu'à là par les scientifiques). Permettent-ils d'augmenter son espérance de gain au loto? Permettent-ils de sortir d'un cercle sans lever le stylo? Permettent-ils de ranger 8 billes dans 7 cases? etc?
- Il est maintenant bien connu qu'on dispose *d'algorithmes aléatoires* qui augmentent **en pratique** l'efficacité des logiciels. Par exemple, on dispose d'un algorithme facile à implémenter, connu depuis longtemps qui nous dit, avec une probabilité qu'on peut faire croitre exponentiellement en fonction des besoins, si un nombre est premier ou non. Cependant, on ne dispose pas **stricto sensu** de générateurs vraiment aléatoires en informatique, du coup on les simule et par un procédé diagonal banal, il est facile de montrer qu'ils échoueront à fournir la mission qu'on attend de vrais tirages aléatoires. En quoi le fait de disposer d'aleas réels et prouvables via les degrés ludiques permettraient-ils de palier à ces manques? Par exemple, la thèse de Church continue-t-elle d'être vraie en présence de téléphones qui réalisent telle ou telle magie?

Dans la suite des sections, on examine quleques problèmes bien connus et on essaie de faire le point sur les niveaux de magie concernés. On traite aussi bien l'aspect Tukey que l'aspect ludique (qui le généralise).

2.14 Colorations de graphes

Dans le cas des graphes finis, c'est une classe de problèmes NP-complets. Nous allons voir que le sujet est riche en invitations canoniques. Tous les graphes considérés dans la section sont non orientés.

Définition 42 *Soit $G := (S, A)$ un graphe. Le degré de Tukey $T(G)$ associé à G dont la définition suit sera appelé nombre chromatique virtuel de G.*

La définition suivante définit $T(G)$:

Définition 43 *On note W l'ensemble des parties X (dites indépendantes) de S telles que $\forall p \in A : p$ n'est pas inclus dans X. $T(G)$ est alors le triplet $(S, W, \in_{S\times W})$.*

Soient G, H deux graphes. Le degré ludique suivant mesure l'éloignement entre la difficulté de colorier G et celle de colorier H.

Définition 44 *Soient $u := (E, F, R)$ et $v := (E', F', R')$ deux relations de Tukey. On note collapse(u, v) la garantie ludique à deux combinés suivante:*
Le clavier du premier combiné est E'. Son écran est E
Le clavier du deuxième combiné est F et son écran est F'
La garantie est l'ensemble des $([q', q], [r, r'])$ tels que $(q, r) \in R$ implique $(q', r') \in R'$

Remarque : . Il est facile de voir que le degré ludique de $collapse(u, v)$ ne dépend que des degrés de Tukey de u et de v.

Vu la définition, il est évident que $collapse(u, v)$ est trivial si et seulement si $u \leq_{Tukey} v$.

Le degré ludique attaché à $collapse(T(G), T(H))$ mesure le niveau de magie qu'il faut pour passer d'un coloriage de G qui serait donné à un coloriage de H. En particulier, s'il est trivial, cela signifie qu'il existe un plongement (pas forcément injectif, ie un morphisme de graphe) de H dans G. En particulier, si on note K_n une clique avec n sommets, on obtient le niveau de magie qu'il y a à colorier un graphe H en considérant le degré ludique $collapse(T(K_n), T(H))$.

Deux remarques sur des différences de résolution

- La borne inférieure Z de $T(G), T(H)$ en tant que degrés de Tukey **n'est pas toujours** égale au degré de Tukey $T(L)$ où L est le graphe produit de G et de H. Par contre: $Z \geq_{Tukey} T(L)$
- De nombreux degrés ludiques peuvent être associés à une même volonté de mesurer la *magie* présente dans un *prodige* selon le point de vue qu'on souhaite adopter. Cela est simplement la conséquence du paradigme téléphonique et des armes qu'on décide de définir pour l'attaque sceptique.

Par exemple, le fait de couvrir l'ensemble des sommets d'un graphe par 15 ensembles indépendants est une attestation qu'il peut être colorié avec 15 couleurs. Mais on peut aussi demander simplement une coloration du graphe avec 15 couleurs. Si, de manière statique, les deux procédures peuvent sembler équivalentes, l'approche sceptique est très différente.

Dans un cas il demande les ensembles indépendants dans leur entier de manière statique alors que dans l'autre, il sera moins sévère et n'aura besoin que de regarder (lors d'un instantané du test) la couleur du sommet qu'il aura choisi. Il est intuitivement presque évident que le deuxième protocole est bien plus confortable pour le prouveur que le graphe objet de la confrontation est coloriable avec 15 couleurs.

Les deux remarques précédentes sont de nature différentes mais viennent se ranger dans la même catégorie d'obstacles à l'unicité des notions (irrémédiable) générées par la présente théorie.

Nous illustrons la deuxième remarque par une définition et plusieurs théorèmes intéressants en soi:

Définition 45 *Soit $G := (S, A)$ un graphe et n un entier. On appelle coloration ludique de G (le degré ludique du) le téléphone à deux combinés défini comme suit:*

- *Les claviers des deux combinés sont S.*
- *Les écrans des deux combinés sont n.*
- *La garantie est l'ensemble des $([x, y], [a, b])$ tels que $(x \neq y$ ou $a = b)$ et $((\{x, y\} \notin A$ ou $a \neq b))$*

Dans le présent paragraphe, on notera $CL(G, n)$ la coloration ludique de G avec n couleurs.

Définition 46 *On appelle nombre chromatique quantique de G le plus petit entier n tel que $CL(G, n)$ soit FMQ*[1]

Le théorèmes de Kochen Specker entraine que le degré ludique quantique d'un graphe peut ne pas être égal à son nombre chromatique réel, comme l'illustre le théorème suivant:

Lemme 47 *Soit G le graphe dont les sommets sont les demi-droites issues de l'origine de l'espace euclidien canonique porté par $\mathbb{R}^3$ et tel que deux demi-droites sont reliées quand elles sont orthogonales. Le nombre chromatique de G est ≥ 4 et $CL(G, 3)$* **n'est pas FMQ**

Par contre,

Théorème 48 *Soit G le graphe dont les sommets sont les demi-droites issues de l'origine de l'espace euclidien canonique porté par $\mathbb{R}^4$ et tel que deux demi-droites sont reliées quand elles sont orthogonales. Le nombre chromatique de G est ≥ 5* **mais par contre** *$CL(G, 4)$* **est FMQ**

La preuve assez courte utilise les quaternions.

La notion qui suit est une troisième notion, et les lemmes précédents montrent qu'elles sont toutes les trois différentes.

Définition 49 *Soit $G := (S, A)$ un graphe. On appelle nombre chromatique géométrique de G le plus petit entier n tel qu'il existe une application f de S dans un espace euclidien réel de dimension n vérifiant: $\forall\{a; b\} \in A : f(a) \perp f(b)$*

Théorème 50 *Pour tout graphe G, si (a, b, c) est le triplet de son nombre chromatique, son nombre chromatique quantique et son nombre chromatique géométrique, alors $a \geq b \geq c$*

2.15 Nécessité des écrans ET des claviers

2.15.1 Introduction

Cette section décrit de quelle manière, d'une part les écrans sont nécessaires pour atteindre un faible niveau de non localité et d'autre part de quelle manière formelle certaines contraintes (comme l'indéterminisme par exemple) sont incompatibles avec la non localité. On va voir en particulier que l'échappatoire, pour un combiné, de l'écran attaché au combiné que son utilisateur a décrété avoir vocation d'émetteur est une réelle option de puissance.

[1] voir définition de degré ludique FMQ au chapitre 8

2.15.2 Rappels de notations

Dans ce chapitre, on utilise les *définitions officielles* de la théorie des ensembles. En particulier $1 = \{\emptyset\}$ et $2 = \{0; 1\}$. Comme dans le reste du texte, $A \to B$ désigne l'ensemble des **applications** de A dans B

2.15.3 Quand un écran est inactif

Soit T un téléphone ludique d'uplicité2 dont l'écran du combiné1 ne sert à rien, c'est à dire, de signature $((E_1 \times F_1) \times (E_2 \times F_2), G)$ tel que:

$$\forall (y_1, z) \in F_1^2, \forall (x_1, x_2, y_2) \in E_1 \times E_2 \times F_2, ((x_1, y_1), (x_2, y_2)) \in G \Rightarrow ((x_1, z), (x_2, y_2)) \in G$$

Lemme 51 *Si T n'est pas trivial alors T est TSD*

Autrement dit, il est impossible d'avoir une non localité non transmettrice d'information sans disposer au minimum de deux écrans **actifs**

Preuve : Soit $a \in F_1$. Supposons que pour toute $f \in (E_2 \to F_2)$, il existe $(x_1, x_2) \in E_1 \times E_2$ tel que $(x_1, a), (x_2, f(x_2)) \notin G$. Par le lemme de l'étoile, il existe $b \in E_2$ et $h \in F_2 \to E_1$ tel que pour tout $x \in E_1; y \in F_2$: si $((x, a), (b, y_2)) \in G$ alors $x \neq h(y_2)$. Il s'ensuit que dans le sens combiné1 vers combiné2, on peut envoyer une Tukey-information de niveau $(E_1, E_1, \neq)$.

2.15.4 Quand un clavier est inactif

Soit T un téléphone ludique d'uplicité2 dont le clavier du combiné2 ne sert à rien, c'est à dire, de signature $((E_1 \times F_1) \times (1 \times F_2), G)$.

Lemme 52 *Si T n'est pas trivial alors T est TSD*

Le bilan de ces deux lemmes est qu'il est impossible d'avoir une non localité non transmettrice d'information sans disposer au minimum de deux claviers ET deux écrans **tous les quatre actifs**

Preuve : Comme $E_2 = 1$, on a donc que pour tout $f \in (E_1 \to F_1)$ et tout $y_2 \in F_2$, il existe $x_1 \in E_1$ tel que $((x_1, f(x_1)), (1, y_2)) \notin G$. Le lemme de l'étoile donne alors qu'il existe $h \in (F_2 \to E_1)$ tel que pour tout $x \in E_1; y_1 \in E_1; y_2 \in E_2$: si $((x_1, y_1), (1, y_2)) inG$ alors $x \neq h(y_2)$ et donc on peut se servir de T pour envoyer un Tukey-$(E_1, E_1, \neq)$ message.

Chapitre 3

Les degrés de Tukey, cas particuliers de degrés ludique

3.1 Précisions de notations

Dans ce chapitre, on admet l'axiome du choix et les cardinaux sont par définition les ordinaux a tels qu'il n'existe pas (b, f) où $b \in a$ et f surjective de b sur a. On rappelle que $\{(x, y) \in a^2 \mid x \in y$ *ou* $x = y\}$ *est un bon ordre sur n'importe quel ordinal* a.

Dans toute la suite on ne s'intéresse qu'à l'uplicité $n := 2$. Mais on ajoute encore d'autres restrictions aux combinés téléphoniques. On s'intéresse aux téléphones à deux combinés (indicés par $2 := \{0; 1\}$), mais qui de plus ont la propriété suivante: *l'écran du combiné1 est de cardinal 1. Le clavier du combiné2 est de cardinal 1.* **Dans ces conditions, l'utilisateur du combiné1 est obligé de se concevoir comme un émetteur et l'utilisateur du combiné2 est obligé de se concevoir comme un récepteur**. Rappel: $1 := \{0\}$

On est face à des téléphones dont la garantie, qui au départ est un ensemble de quadruplets inclus dans $(E \times 1) \times (1 \times F)$, peut se concevoir comme une partie de $E \times F$ et on a le théorème évident suivant:

Théorème 53 *Soient* $a := ((E \times 1) \times (1 \times F), G)$ *et* $b := ((E' \times 1) \times (1 \times F'), G')$ *deux garanties ludiques d'uplicité 2. Alors* $a \leq_{ludique} b$ *si et seulement s'il existe* $f \in (E \to E')$ *et* $g \in (F' \to F)$ *telle que pour tous* $x \in E$*, tout* $y \in F'$ *si* $([f(x), 0], [0, y]) \in G'$ *alors* $([x, 0], [0, g(y)]) \in G$

On obtient exactement une notion connue (depuis les années 1940) sous le nom de *réduction de Tukey.*

3.2 Résumé et lemmes de base sur les degrés de Tukey

Nous noterons indifféremment $E \to F$ ou F^E l'ensemble des applications d'un ensemble E dans un ensemble F. Soient E, F, G, H quatre ensembles et $R \subseteq E \times F$ et $S \subseteq G \times H$.

Définition 54 *La notation* $(E, F, R) \leq_{tuk} (G, H, S)$ *abrège l'énoncé suivant:*

$$\exists f \in E \to G, \exists g \in H \to F : \forall x \in E, \forall r \in G, (f(x), y) \in S \Rightarrow (x, g(y)) \in R$$

Quand $X := (E, F, R)$, *on note* $Entree(X) := E; Sortie(X) := F; Garantie(X) := R$. *Le couple* (f, g) *dont l'existence est en jeu s'appellera un témoin de réduction de Tukey de* (E, F, R) *à* (G, H, S)

Cette définition est classique, mais l'introduction historique des degrés de Tukey n'a pas été motivée par la démarche que nous décrivons maintenant.

3.2.1 Degré de Tukey comme mesurant des qualités de téléphones

- Un triplet tel que le (E, F, R) ci-dessus représente **un niveau de qualité téléphonique**.
- L'ensemble E peut être vu comme **le clavier** d'un téléphone, l'ensemble F comme un ensemble de configurations d'écran possible. De manière plus abrégée, nous l'appelons **l'écran du téléphone**.
- L'ensemble $R \subseteq E \times F$ peut être regardé comme une **garantie constructeur** qui s'exprimerait comme suit: *quand vous taperez sur la touche* $x \in E$ *de votre clavier, je vous garantis que vous recevrez un* y *à l'écran tel que* $(x, y) \in R$, *ni plus ni moins. En particulier, le constructeur ne vous dit rien de "la boite noire" qui enverra le message du combiné emetteur au combiné récepteur, ni de la dégradation possible durant le trajet de l'information si toutefois celle-ci avait un sens*
- Le couple (f, g) éventuel qui témoigne une réduction de a à b est un procédé de simulation d'un téléphone a-garanti quand on dispose d'un téléphone b-garanti.
- La *distance* mathématique abstraite entre l'émetteur et le récepteur est souvent symbolisée par la petite barre verticale dans les démonstrations. Dans le paradigme de Tukey, l'équipe Alice-Bob tente de communiquer **en sens unique et avec un seul message**, de Alice vers Bob

Lorsque R n'est pas incluse dans $E \times F$, on considère tacitement que le triplet (E, F, R) représente la relation $(E, F, R \cap (E \times F))$.

Nous pouvons voir ainsi **n'importe quel triplet d'ensembles** comme un représentant "de Tukey", et étendre le préordre à tous ces triplets.

Le lemme de base est que la réduction de Tukey est transitive:

Lemme 55 $\leq_{tuk}$ *est transitive*

Preuve : On dessine:

$$x \to f(x) \to f'(f(x)) \mid z \to g'(z) \to g(g'(z))$$

qui schématise comment enchainer des simulations. Si (f, g) est un témoin de réduction de a à b et (f', g') est un témoin de réduction de b à c alors $(f' \circ f, g \circ g')$ est un témoin de réduction de a à c

Définition 56 *La relation*

$$(E, F, R) ==_{tuk} (E', F', R')$$

définie par

$$(E, F, R) \leq_{tuk} (E', F', R') \text{ et } (E', F', R') \leq_{tuk} (E, F, R)$$

est une relation d'équivalence qui sera notée également $==_T$ *ou* $==_{tukey}$

Les classes sont à priori des collections, et on les appelle: **les degrés de tukey**

Ce paradigme, ou plutôt cette façon de "regarder" les degrés de Tukey et leurs représentants rend évident (modulo l'axiome du choix) le théorème suivant:

Théorème 57 *Soit* (E, F, R) *un triplet "de Tukey". Il existe* $S \subseteq P(E)$ *tel que*

$$(E, S, \in) ==_T (E, F, R)$$

En outre, on peut choisir S *stable par passage aux sous-ensembles, ie tel que*

$$\forall X, Y : ((X \in S \textit{ et } Y \subseteq X) \textit{ implique } Y \in S)$$

Afin de familiariser le lecteur avec le paradigme téléphonique, nous écrivons deux preuves, l'une plus informelle mais mettant en avant l'aspect téléphonique.

Preuve :

- preuve informelle: Pour les utilisateurs d'un (E, F, R)-téléphone, lorsque le récepteur lit $y \in F$ sur son écran, l'information qu'il récupère sur le x qui a été joué par l'émetteur est que $x \in D(y) := \{e \in E \mid (e, y) \in R\}$. On comprend donc bien que, finalement, seul compte pour le récepteur cet ensemble $D(y)$
- Preuve plus formelle: Soit S l'ensemble des $D(y)$ quand y parcourt F. Montrons que $(E, S, \in) ==_T (E, F, R)$. Soit $(x, y) \in R$. Alors $(x, D(y)) \in S$. Il s'ensuit que la stratégie

  $$x \to x \mid y \to D(y)$$

  atteste que $(E, S, \in) \leq_{tuk} (E, F, R)$.
  Réciproqement, soit g telle que $\forall z \in F : D(g(D(z))) = D(z)$ (utilisation de l'axiome du choix) et supposons que $x \in A \in S$. Il existe alors $y \in F$ tel que $A = D(y)$ et $x \in A$.
  Soit $z := g(A)$. Alors $D(z) = D(y)$ et $x \in D(z)$ donc $(x, z) \in R$. Par conséquent la stratégie

  $$x \to x \mid A \to g(A)$$

  atteste que $(E, F, R) \leq_{tuk} (E, S, \in)$

Le lemme suivant achève la démonstration du théorème:

Lemme 58 *Soit* $a := (E, S, \in)$ *un représentant de Tukey tel que* $S \subseteq P(E)$. *On note*

$$S' := \{X \mid \exists Y \in S : X \subseteq Y\}$$

Alors

$$b := (E, S', \in) ==_{tuk} (E, S, \in)$$

Preuve : Nous dessinons la réduction: la barre verticale représente la séparation entre émetteurs et récepteurs. Les flèches représentent les stratégies de simulation.

$$x \in E \to x \mid A \in S \to A(\in S')$$

est une réduction de Tukey de a à b.

Réciproquement: soit $\phi \in (S' \to S)$ telle que $\forall X \in S' : X \subseteq \phi(X) \in S$, alors la réduction de b à a peut être dessinée comme suit:

$$x \in E \to x \mid X \in S' \to \phi(X)$$

3.2.2 Quelques précisions sur ce genre de schéma

Soient (E, F, R) et (E', F', R') des représentants de degrés de Tukey. Il semble commode de décrire une réduction du premier au deuxième par un petit dessin de la forme:

$$x \to f(x) \mid y \to g(y)$$

sans préciser les ensembles de départ et d'arrivée quand aucune confusion n'est possible.

S'il y a risque de confusion, on écrira plutôt:

$$x \in E \to f(x) \in E' \mid y \in F' \to g(y) \in F$$

Il pourra aussi arriver parfois que nous omettions **certains** ensembles de départ ou d'arrivée, mais pas tous, comme par exemple:

$$x \in E \to f(x) \mid y \in F' \to g(y) \in F$$

D'une manière générale, quand on veut vraiment éviter toute forme d'ambiguité, on écrit toutes les mentions:

$$X : [x \in Entree(X) \to f(x) \in Entree(Y) \mid y \in Sortie(Y) \to g(y) \in Sortie(X)]$$

qui signifie:

$$\forall (x, y) \in Entree(R) \times Sortie(S), (f(x), y) \in S \Rightarrow (x, g(y)) \in R$$

en notant $R := Garantie(X)$ et $S := Garantie(Y)$, c'est à dire $X \leq_{tuk} Y$

3.2.3 Convention Alice-Bob

Nous avons titré cette sous-section ainsi pour que la table des matières y conduise rapidement le lecteur. Une des conventions que nous utiliserons souvent est de nommer Alice comme utilisateur **émetteur** d'un téléphone et Bob comme utilisateur récepteur.

L'équipe qu'ils formeront sera souvent amenée à simuler un téléphone à partir d'autre(s) ou à réussir une communication à distance (une distance abstraite).

3.2.4 Autre représentant canonique

Le théorème suivant a une utilité quand, par exemple, avec l'axiome du choix, on souhaite un représentant d'un degré qui soit un sous-ensemble de a^2 où a est un cardinal ou un ordinal.

Théorème 59 *Soit (E, F, R) un triplet "de Tukey". Il existe alors un ensemble G et $S \subseteq G \times G$ tel que $(E, F, R) ==_T (G, G, S)$. On peut choisir pour G un cardinal, en envoyant tout par une bijection de G sur $card(G)$*

Preuve : On peut supposer que $F \subseteq P(E)$ et que $R = \in_{E \times F}$ d'après le théorème précédent. Il suffit alors de prendre $G := P(E)$ et de considérer $S := \{(A, B) \in G^2 \mid$ si A est un singleton de la forme $\{x\}$ alors $x \in B$ et $B \in F\}$. Voici la réduction obtenue dans un sens:

$$x \in E \to \{x\} \mid A \in G \to A$$

Et dans l'autre sens:

$$A \in G \to x(A) \in E \mid B \in G \to B$$

où on a au préalable choisi $A \mapsto x(A)$ telle que pour tout $t \in E : x(\{t\}) = t$

3.2.5 Dualité

Une des qualités des degrés de Tukey est qu'ils sont munis naturellement d'une opération qui joue un rôle dualisant:

Définition 60 *Soit $X := (E, F, R)$. On note X^* le triplet (F, E, S) où*

$$S = \{(x, y) \in F \times E \mid (y, x) \notin R\}$$

.

Cette opération **n'a pas** son analogue pour les cardinaux

Théorème 61 *Pour toutes relations de Tukey*

$$X, Y : (X^*)^* = X \text{ et } (X \leq_{tuk} Y \iff Y^* \leq_{tuk} X^*)$$

Preuve : La première affirmation est évidente, la deuxième vient du fait que le dessin et ses sous-entendus:

$$X : [x \to f(x) \mid_Y y \to f(y)]$$

signifie que le couple (f, g) est une réduction de Tukey X à Y ce qui revient au même que de dire:

$$Y^* : [y \to g(y) \mid_{X^*} x \to f(x)]$$

puisque

$$\forall (x, y) \in E \times F' : ((f(x), y) \in S \Rightarrow (x, g(y)) \in R) \iff ((x, g(y)) \notin R \Rightarrow (f(x), y) \notin S)$$

Nous verrons dans la section suivante, qui entre un peu plus dans les détails, qu'on peut additionner les degrés de Tukey, les multiplier, et que tout ensemble de degrés de Tukey, a une borne supérieure et une borne inférieure.

En fait, les degrés de Tukey **généralisent la notion de cardinal**

Parfois, il sera utile de considérer des (E, F, R) où $E = F$ alors que d'autres fois on préfèrera plutôt des représentants de la forme $(E, S, \in)$ où $S \subseteq P(E)$).

Voici quelques exemples de degré de Tukey :

3.2.6 Exemples de degrés de Tukey

Les degrés de tukey généralisent les cardinaux d'une manière presque évidente une fois qu'on s'est mis d'accord avec la présentation des Tukey comme des *quantités d'informations* ou encore des *mesures de puissance téléphonique.*

Définition 62 *Soit c un ensemble. On note I_c le degré de Tukey de $(c, c, =)$ ou si le contexte n'induit pas d'ambiguité, le triplet $(c, c, =)$ lui-même sera éventuellement abrégé en c tout court, au lieu de I_c. Quand il y a peu de risque de confusion, il arrive aussi que l'on note le degré de Tukey de I_c par son représentant I_c lui-même.*

Le théorème suivant, indique que $c \mapsto I_c$ plonge les cardinaux dans les degrés deTukey.

Théorème 63 *Soient c, d des cardinaux: alors $c \leq_{card} d$ si et seulement si $I_c \leq_{Tuk} I_d$.*

Preuve : Notons $f : c \to d$ définie par $f(x) = x$ si $x \in d$ et $f(x) = 0$ sinon, et g la fonction défnie de la même façon en permutaut c et d. Dessinons les réductions:

$$x \in c \to f(x) \in d \mid y \in d \to g(y) \in c$$

qui montre que si $c \leq d$ alors $I_c \leq_{tuk} I_d$

Supposons que $I_c \leq_{Tuk} I_d$ soit attesté par une réduction

$$x \in c \to f(x) \in d \mid y \in d \to g(y) \in c$$

Cela entraine que $\forall (x, y) \in c \times d$: si $f(x) = y$ alors $x = g(y)$, ce qui se récrit en disant que $g \circ f = id_c$ et donc que f est une **injection** de c dans d

En fait, la preuve précédente révèle un théorème plus général:

Théorème 64 *Soient des ensembles e, u* **quelconques**. *Les conditions suivantes sont équivalentes:*

- $I_e \leq_{tuk} I_u$
- $card(e) \leq card(u)$

Ce théorème illustre bien l'annonce: *les degrés de Tukey généralisent les cardinaux*

Les degrés de Tukey suivants joueront un rôle crucial dans l'étude de **l'éternité**[1].

[1] voir chapitre 6

Définition 65 *Soit c un ensemble. D_c est, par définition, le degré de Tukey de $(c, c, \in)$*

Remarque : Il est facile de voir que si c est un ordinal limite, alors $(c, c, \in) ==_{tuk} (c, c, \leq)$, ce qui permet de dire que D_c est auto-dual (i.e. son propre dual).

Il suffit de parcourir tous les cardinaux infinis réguliers pour avoir la collection de tous les degrés des $(a, a, \in)$ quand a parcourt les ordinaux limite. Cela a peut-être été une des premières motivations historiques des degrés de Tukey:

Lemme 66 *Pour tout ordinal limite a, il existe un cardinal régulier c tel que $(a, a, \in) ==_{Tukey} (c, c, \in)$ et c est la cofinalité de a*

Preuve : Soit f une application strictement croissante de $c \to a$ dont l'image est cofinale dans a. Soit h allant de a dans c telle que $\forall x \in a$: le plus petit $y \in c$ tel que $f(y) \geq x$ est strictement inférieur à $h(x)$

Alors la stratégie

$$x \to f(x) \mid y \to h(y)$$

atteste que $(c, c, \in) \leq (a, a, \in)$ et réciproquement la stratégie

$$x \to h(x) \mid y \to f(y)$$

atteste que $(a, a, \in) \leq (c, c, \in)$

La preuve précédente donne en fait plus:

Théorème 67 *Soit $(E, \leq)$ un ensemble totalement ordonné sans maximum. Il existe alors un unique cardinal régulier c tel que $(c, c, \in) ==_{Tukey} (E, E, \leq)$. Ce cardinal s'appelle* **la cofinalité de** $(E, \leq)$

Preuve : même preuve que dans le cas particulier du lemme, où l'ordre est $(a, \in)$ avec a ordinal limite, en prenant $c :=$ le plus petit cardinal infini e tel qu'il existe une application strictement croissante de e dans E, dont l'image n'est pas bornée

Autrement dit, du point de vue des degrés de Tukey, la bonne fondation d'un ordre total est invisible sur son degré de Tukey.

Définition 68 *On note $BottomTukey$ (ou en plus abrégé, si pas de risque de confusion : $Bottom$) le degré de I_1*

Les deux degrés suivants jouent les rôles de maximum et de minimum de la collection ordonnée des degrés de Tukey:

Théorème 69 *I_1 (son degré de Tukey) est le plus petit de tous les degrés de Tukey. $TopTukey := I_1^*$ est le plus grand de tous les degrés de Tukey. Il pourra arriver parfois qu'on les note $InfiniTukey$ au lieu de $TopTukey$ et $UnTukey$ au lieu de $BottomTukey$*

N'importe quel triplet $v := (E, F, R)$ tel que $\exists x \in E : \forall y \in F, (x, y) \notin R$ vérifie $degredeTukey(v) = TopTukey$ (ou Top si pas de risque de confusion)

Dualement, n'importe quel triplet $v := (E, F, R)$ tel que $\exists y \in F : \forall x \in E, (x, y) \in R$ vérifie $degredeTukey(v) = BottomTukey$

3.3 Approfondissements

Les définitions et théorèmes de base concernant les degrés de Tukey ont été donnés dans les sections précédentes.

Nous avons affirmé qu'ils généralisaient les cardinaux. Nous approfondissons dans les sections suivantes cette idée et structurons la collection des degrés de tukey avec des opérations d'addition, de produits, de borne inférieure et supérieure. On remarquera aussi l'intéressante existence de degrés "indivisibles" dans un sens qui sera précisé.

Tout d'abord, à chaque degré de Tukey, on peut associer deux cardinaux naturels, sa cofinalité et la cofinalité de son dual:

Définition 70 *Soit $v := (E, F, R)$ une relation non TopTukey. On appelle cofinalité de v le plus petit des cardinaux c tel que $I_c \geq_{Tukey} v$.*

Remarque : Il est évident qu'un tel cardinal existe car $I_{card(E)} \geq_{Tukey} v$

Attention: il n'y a pas de raison que la cofinalité d'un Tukey soit un cardinal régulier, comme le montre l'exemple de la cofinalité de I_κ qui ne peut être que κ lui-même

Théorème 71 *La cofinalité de v ne dépend que du degré de Tukey de v*

La preuve de ce théorème est une conséquence du lemme:

Lemme 72 *Soient a, b des représentants de Tukey (c'est à dire des triplets). Alors si $a \leq_{tuk} b$ alors $cof(a) \leq cof(b)$*

Preuve : La relation $\leq_{tuk}$ est transitive d'où $a \leq_{tuk} b \leq_{tuk} I_c$ entraine que c est au moins aussi grand que la cofinalité de a

3.4 Bornes supérieures

Comme il a été signalé plus haut, pour tout degré de Tukey d, il existe un représentant de la forme (E, E, R) dans d. En fait, on dispose de mieux:

Théorème 73 *Soit $i \in J \mapsto (E_i, F_i, R_i)$. Il existe un ensemble T et $i \mapsto S_i$ vérifiant*

$$\forall i \in J : (E_i, F_i, R_i) ==_{Tukey} (T, T, S_i)$$

La preuve est une fois de plus légèrement cabalistique, mais le paradigme téléphonique rend le phénomène évident: en effet, on peut ne pas changer la puissance d'un téléhpone en agrandissant son clavier, et en convenant que les touches rajoutées ne servent à rien et en agrandissant son écran et en convenant que les éléments rajoutés n'ont aucune signification particulière et n'apparaissent pas quand un "bonne touche" (non rajoutée pour décorer) est appuyée, bien qu'ils fassent "officiellement" partie des lampes de l'écran. C'est le sens de l'ensemble F dont l'existence est affirmée.

Preuve : On montre que pour toute famille de $(E_i, F_i, R_i), i \in J$ il existe une famille de $(F, F, S_i), i \in J$ telle que pour tout $i \in J$ le degré de Tukey de (E_i, F_i, R_i) est le même que celui de (F, F, S_i)

Soit un ensemble F tel que $\forall i \in J : E_i \cup F_i \subseteq F$. Posons $S_i := \{(x, y) \in F^2 |$ si $x \in E_i$ alors $y \in F_i$ et $(x, y) \in R_i\}$. Alors $(F, F, S_i) ==_{Tukey} (E_i, F_i, R_i)$. Soit $i \in J$: Voici les stratégies de réductions:

$$x \in E_i \mapsto x \in F \mid y \in F_i \to y \in F$$

dans un sens et,

$$x \in F \to f(x) \mid y \in F \to g(y) \in F$$

dans l'autre sens, où pour construire f, g, on choisit n'importe quels éléments e, u respectivement dans E_i, F_i et on pose $f : x \in E_i \mapsto x$ et $f : x \notin E_i \mapsto e$ et $g : y \in F_i \mapsto y$ et $g : y \notin F_i \mapsto u$.

On va donc pouvoir étudier la question de la borne supérieure en supposant que tous les degrés sont représentés par un triplet (E, E, R_i) où E est le même pour tous, aussi bien comme clavier que comme écran.

Théorème 74 *Soit $a_i, i \in J$ des degrés de Tukey. Il existe un degré de Tukey b tel que:*

- *$\forall i \in J : b \geq_{tuk} a_i$ et*
- *Pour tout degré c, si $\forall i \in J : c \geq_{tuk} a_i$ alors $c \geq_{tuk} b$*

Preuve : On peut supposer qu'on a comme famille $i \in J \mapsto v_i := (E, E, R_i)$, d'après le théorème précédent. Posons $D := J \times E$, $A := J \to E$ et $S := \{((i, x), f) \in D \times A \mid (x, f(i)) \in R_i\}$. On pose $w := (D, A, S)$. La stratégie

$$x \to (i, x) \mid f \to f(i)$$

atteste que $v_i \leq w$. Il s'ensuit que w majore la famille $i \mapsto v_i$. Soit $m = (G, G, T)$ un majorant de cette famille. Il existe des stratégies $x \in E \to g_i(x) \in G \mid y \in G \to h_i(y) \in E$ telles, pour chaque $i \in J$, que $\forall x \in E \forall y \in G$: si $(g_i(x), y) \in T$ alors $(x, h_i(y)) \in R_i$. La stratégie qui suit réduit w à m:

$$(i, x) \to g_i(x) \mid y \to K(y)$$

où $K(y)$ est l'application de J dans E définie par $K(y)(j) := h_j(y)$

Autrement dit, tout ensemble de degrés de Tukey a une borne supérieure. Par dualité, on en déduit : Tout ensemble de degrés de Tukey a une borne inférieure

Remarque : Les considérations précédentes *passent au quotient* et finalement ne concernent que les degrés de tukey et non leurs représentants.

3.5 Sommes et produits

Dans cette section, $i \in J \mapsto v_i := (E, E, R_i)$ désigne une famille de triplets représentant des degrés de Tukey. On va définir la somme et le produit de cette famille.

Définition 75 *Notons $A := J \times E$. Soit S l'ensemble des $((i, x), (j, y))$ de A^2 tels que $i = j$ et $(x, y) \in R_i$. Le triplet (A, A, S) sera appelée la somme des v_i.*

Dans le cas général d'une famille $v_i := (E_i, F_i, R_i)$, la somme est définie par le triplet (D, A, S) où:

- $D :=$ l'ensemble des couples (i, x) tels que $x \in E_i$ et $i \in J$

- $A :=$ l'ensemble des couples (i, x) tels que $x \in F_i$ et $i \in J$
- $S :=$ l'ensemble des $((i, x), (j, y))$ tels que $i = j$ et $(x, y) \in R_i$

Il s'agit, là encore, d'une notion qui passe au quotient. Autrement dit:

Théorème 76 *Si $\forall i \in J : v_i \leq_{Tukey} w_i$ alors la somme des $v_i, i \in J$ est $\leq_{Tukey}$ à la somme des $w_i, i \in J$*

Preuve : Soient f_i, g_i des stratégies

$$x \to f_i(x) \mid y \to g_i(y)$$

qui réduisent les v_i aux w_i. Alors la stratégie

$$(i, x) \to (i, f_i(x)) | (j, y) \to (j, g_j(y))$$

réduit la somme des v_i à la somme des w_i

Définition 77 *Notons $A := E^J$ et $P := \{(x, y) \in A^2 \mid \forall i \in J : (x(i), y(i)) \in R_i\}$*
Le triplet (A, A, P) sera appelée le produit des v_i.

Il s'agit, là encore, d'une notion qui passe au quotient. Autrement dit:

Théorème 78 *Si $\forall i \in J : v_i \leq_{Tukey} w_i$ alors le produit des $v_i, i \in J$ est $\leq_{Tukey}$ au produit des $w_i, i \in J$*

Preuve : Soient f_i, g_i des stratégies

$$x \to f_i(x) | y \to g_i(y)$$

qui réduisent les v_i aux w_i. Alors la stratégie

$$x \to (i \mapsto f_i(x(i))) \mid y \to (i \mapsto g_i(y(i)))$$

réduit le produit des v_i au produit des w_i

Remarque : Nous n'avons pas défini de la manière la plus générale possible ce que signifie *le produit des* (E_i, F_i, R_i) quand $i \mapsto (E_i, F_i)$ n'est pas constante. Ce qui nous intéresse est le passage au quotient. La définition générale se devine aisément. Le produit de représentants correspond au produit des **garanties téléphoniques** qui lui-même correspond à la garantie qui définit **le droit d'utiliser tous les téléphones de la famille**.

3.6 Propriétés annelées

Donnons un théorème dont l'énoncé sera précisé par les lemmes qui jalonneront le détail de sa preuve:

Théorème 79 *Les sommes et produits ainsi définis sur les degrés de Tukey sont commutatives et associatives, la commutativité étant dans le sens fort, puisque les définitions donnent directement des sommes et produits quelconques, donc entre autre avec un nombre infini de termes. De plus la multiplication est distributive par rapport à l'addition.*

Preuve du théorème

Lemme 80 *La somme est commutative*

Preuve : Soient des degrés de Tukey d_i pour lesquels nous avons choisi une famille de représentants (E, E, R_i), quand i parcourt J. soit σ une permutation de J. On souhaite prouver que la somme des d_i est égale à la somme des $d_{\sigma(i)}$. Remarquons que la famille $i \mapsto (E, E, R_{\sigma(i)})$ représente la famille de degrés $d_{\sigma(i)}$. La stratégie

$$(i, x) \to (\sigma(i), x) \mid (j, y) \to (\sigma^{-1}(j), y)$$

réduit la somme des (E, E, R_i) à la somme des $(E, E, R_{\sigma(i)})$

Lemme 81 *Le produit est commutatif*

Preuve : Soient des degrés de Tukey d_i pour lesquels nous avons choisi une famille de représentants (E, E, R_i), quand i parcourt J. soit σ une permutation de J. On souhaite prouver que le produit des d_i est égal au produit des $d_{\sigma(i)}$. Remarquons que la famille $i \mapsto (E, E, R_{\sigma(i)})$ représente la famille de degrés $d_{\sigma(i)}$. La stratégie

$$x \to (x \circ \sigma)|y \to (y \circ \sigma^{-1})$$

réduit le produit des (E, E, R_i) au produit des $(E, E, R_{\sigma(i)})$. En effet, si $\forall i : (x(\sigma(i)), y(i)) \in R_{\sigma(i)}$, c'est à dire si $(x \circ \sigma, y)$ appartient au produit des $R_{\sigma(i)}$ alors $\forall i : (x(i), y(\sigma^{-1}(i)))$ appartient à R_i et donc le couple $(x, y \circ \sigma^{-1})$ appartient au produit des R_i.

Lemme 82 *La somme est associative*

Preuve : Le cadre notationnel est lourd. On dispose d'une famille $L := i \in J \mapsto (E(i), F(i), R(i))$ de relations qui sont elles-mêmes des sommes de $(G(i, j), H(i, j), S(i, j))$ quand j parcourt $A(i)$. On souhaite montrer que la somme des $(G(i, j), H(i, j), S(i, j))$ quand le couple (i, j) parcourt $\{(i, j) \mid i \in J \text{ et } j \in A(i)\}$ est Tukey-équivalente à la somme de$L$. Nous décrivons les stratégies de réduction sans plus de commentaire:

- $(i, (e, x)) \to ((i, e), x) \mid ((j, u), y) \to (j, (u, y))$
- $((i, e), x) \to (i, (e, x)) \mid (j, (u, y)) \to ((j, u), y)$

Lemme 83 *Le produit est associatif*

Preuve : Nous décrivons les stratégies de réduction sans plus de commentaire en laissant au lecteur le soin de remettre les types correctement:

- $x \to [((i, j) \mapsto x(i)(j)] \mid y \to [i \mapsto (j \mapsto y(i, j))]$
- $x \to [i \mapsto (j \mapsto x(i, j))] \mid y \to [((i, j) \mapsto y(i)(j)]$

Lemme 84 *Soit a un degré de tukey et $i \in J \mapsto x_i$ une famille de degrés de Tukey. Alors $a.(\sum_i x_i) = \sum_i (a.x_i)$*

Preuve : Nous nous contentons de décrire les stratégies de réduction.

$$(0 \mapsto x(0); 1 \mapsto (x(1) = (i, t))) \to (i, (0 \mapsto (x(0)); 1 \mapsto t)) \mid (j, y) \to ((0 \mapsto y(0)); (1 \mapsto (j, y(1))))$$

L'autre sens est analogue

3.7 Conclusion et considérations téléphoniques

Comme avec les cardinaux, les Tukey représente en quelque sorte, la puissance d'un téléphone ou d'une case mémoire d'un ordinateur. Curieusement, mais naturellement, le degré 1 est celui des téléphones qui ne sont d'aucune utilité, de la même manière qu'une case mémoire qui ne peut contenir qu'une seule valeur ne permet pas de stocker de l'information.

Pourtant, en additionnant cette unité "inutile", on obtient de l'information tout à fait respectable. Un téléphone dont vous êtes sûr que si vous tapez sur n'importe quelle touche, le récepteur verra un "bip" s'afficher sur l'écran est équivalent à la donnée de deux objets complètement déconnectés dont l'un, le "récepteur" est simplement un tableau peint par l'artiste du coin, sur lequel apparait un gros "bip" blanc sur fond noir.

Pourtant, de la même manière que $1 + 1 = 2$, les téléphones garantissant $(2, 2, =)$ (dont le degré de Tukey est celui de I_2) permettent d'envoyer des bits d'information (un par téléphone). Il ne faut donc pas concevoir la somme de degrés de tukey comme signifiant quelque chose de matériel. Le produit correspond lui à une action matérielle, consistant à utiliser les deux téléphones.

L'échelle commence à I_1 et continue ainsi de se graduer, comme l'échelle des cardinaux, à la différence près qu'elle n'est pas totalement ordonnée.

Muni des opérations habituelles d'addition et de multiplication des cardinaux, la collection des cardinaux se plonge dans les Tukey isomorphiquement (et canoniquement) de la manière suivante:

Théorème 85 *La fonction j qui envoie un cardinal c sur I_c vérifie: $j(\sum_i c_i) ==_{Tukey} \sum_i j(c_i)$ et $j(\prod_i c_i) ==_{Tukey} \prod_i j(c_i)$, les signes $\sum, \prod$ signifiant respectivement "somme cardinale", "produit cardinal" quand ils sont mis entre des cardinaux, et "somme Tukey", "produit Tukey", quand ils sont mis entre des degrés de Tukey.*

Preuve : La preuve est laissée au lecteur qui remarquera que les I_c ne sont rien d'autre que des représentants de toutes les $(E, E, =)$ possibles.

3.8 Plongement des Tukey dans les ludiques

Soit (E, F, R) une relation de tukey (que l'on note encore R).

Définition 86 *la garantie téléphonique associée à R est la garantie téléphonique d'uplicité2 suivante:*

- *Son entrée Entree est $[E \times 1]$*
- *Sa sortie Sortie est $[1 \times F]$*
- *sa garantie est l'ensemble des $((x, 1), (1, y)) \in Entree \times Sortie$ tels que $(x, y) \in R$*

La relation ludique ci-dessus sera notée $pl(R)$

Soit $L := (E, S, R)$ une relation ludique d'uplicité2.

Définition 87 *On note $permut(L) := (Entree, Sortie, G)$ la relation obtenue par: $Entree(0) := E(1)$ et $Entree(1) := E(0)$ et $Sortie(0) := S(1)$ et $Sortie(1) := S(0)$ et $G :=$ l'ensemble des (q,r) tels que $(q', r') \in R$ où $x'(i) := x(1-i)$ pour chaque $i \in 2,\ x \in \{q, r\}$.*

La définition cabalistique précédente, n'est rien d'autre que l'opération qui consiste à échanger les deux combinés téléphoniques. Curieusement,le passage de la dualité de Tukey à la dualité ludique exige cet échange.

Théorème 88 *Etant données des relations de Tukey R, S quelconques, on a:*

- *$R \leq_{Tukey} S$ si et seulement si $pl(R) \leq_{ludique} pl(S)$ et,*
- *$duale_{ludique}(pl(R)) = permut(pl(dual_{Tukey}(R)))$*

Preuve : Soit $x \to f(x) \mid y \to g(y)$ une stratégie de réduction de R à S. Nous décrivons la stratégie de réduction ludique de $pl(R)$ à $pl(S)$:

- Sur le premier combiné, $x \to f(x) \mid 0 \to 0$
- Sur le deuxième combiné, $0 \to 0 \mid y \to g(y)$

Supposons maintenant que $pl(R) \leq_{ludique} pl(S)$. On a donc une stratégie ludique de la forme suivante:

- Sur le premier combiné, $x \to f(x) \mid 0 \to 0 =: h(x, 0)$
- Sur le deuxième combiné, $0 \to 0 \mid y \to g(0, y)$

qui donne la stratégie de réduction de R à S suivante: $x \to f(x) \mid y \to g(0, y)$

Analysons maintenant la question de la dualité. On a une relation (E, F, R) et notons $T := (pl(R))^*$ le dual de sa garantie ludique canoniquement associée.

Le format de son premier combiné est $1^E \times E$. Le format de son deuxième combiné est $F^1 \times 1$

La garantie est l'ensemble des (f, x) tels que $([x(0), x(1)], [f(0)(x(0)), f(1)(x(1))]) \notin pl(R)$, c'est à dire tels que $(x(0), f(1)(x(1))) \notin R$.

Il faut noter que $f(0)$ est de toute façon l'unique élément de 1^E et que $x(1) = 0$ l'unique élément de 1. Ce téléphone est donc équivalent au téléphone dont la garantie est donnée par $pl(R^*)$ **après échange des deux combinés**

3.9 "Pseudo-plongement" des ludiques dans les Tukey

La réduction ludique est incomparablement plus riche et fine que celle de Tukey. Il parait donc difficile d'analyser les degrés ludiques en attachant chacun des degrés ludiques à un degré de Tukey canonique et en regardant chaque degré ludique à travers son attaché canonique.

Il n'en est pas moins vrai qu'il y a quand-même un Tukey associable canoniquement à **n'importe quel** degré ludique de **n'importe quelle uplicité**.

Soit donc $v := (E, S, G)$ une relation ludique d'uplicité n (la lettre n désigne un ensemble quelconque). L'ensemble E est donc le produit d'une famille $i \in n \mapsto E_i$ et de même pour S. On note M l'ensemble des applications **locales** de E dans S, et on note R l'ensemble des couples $(x, f) \in E \times M$ tels que $(x, f(x)) \in G$

Définition 89 *Le triplet (E, M, R) est par définition la garantie de Tukey attachée à la garantie ludique (E, S, G). On la notera $Tuk(v)$*

On a le théorème suivant:

Théorème 90 *si $u \leq_{ludique} v$ alors $Tuk(u) \leq_{Tukey} Tuk(v)$*

Preuve : Soit f, g des stratégies resp locales, bilocales de réduction de u à v:

$\lambda i : x_i \to f_i(x) \mid y_i \to g_i(x_i, y_i)$

La stratégie suivante réduit $Tuk(u)$ à $Tuk(v)$:

$x \mapsto (i \mapsto f_i(x(i))) \mid (i \mapsto h_i) \to (i \mapsto (z \mapsto g_i(z, h_i(f_i(z)))))$

On en déduit de façon immédiate que si $u ==_{ludique} v$ alors $Tuk(u) ==_{Tukey} Tuk(v)$, la réciproque étant fausse. Dès lors, on peut se demander dans quelle mesure la relation $(u, v) \mapsto Tuk(u) ==_{Tukey} Tuk(v)$ est une bonne approximation de $==_{ludique}$? Nous n'avons pas approfondi cette question.

Chapitre 4

Quelques exemples

Soit X un ensemble. Dans ce chapitre, nous utiliserons la notation $\in_X = \{(x, y) \in X \mid x \in y\}$. En général X est un ensemble produit de la forme $E \times F$. Nous exposons dans ce chapitre une liste d'exemples, dont certains sont anecdotiques, mais d'autres sont importants dans la suite de ce texte.

4.1 Injection Virtuelle

Comme dit dans l'introduction, une des raisons d'être, si ce n'est la raison d'être, des degrés ludiques est de mesurer "la magie" nécessaire et suffisante pour obtenir des "impossibilités".

On donne donc les définitions des "injections virtuelles" d'un cardinal dans un autre et, plus généralement, d'un degré de Tukey dans un autre.

Soit n, p deux cardinaux. Le téléphone suivant est appelé *injection virtuelle de n dans p*:

- C'est un téléphone à deux combinés.
- Le clavier du premier combiné est n.
- Le clavier du deuxième combiné est p.
- L'écran du premier combiné est p.
- L'écran du deuxième combiné est n.
- La garantie est l'ensemble des $((q, r), (r', q'))$ tels que $q = q'$ ou $r \neq r'$

Ce téléphone sera noté $Injvirt(n, p)$. Il est évidemment bottomludique ssi $n \leq p$

Remarque : Il est assez facile de voir que si $n > p > 1$, Injvirt(n,p) est non TSD et non triviale. La définition de TSD est donnée dans le chapitre précédent.

.

Plus généralement, étant donné $n := (E, F, R)$, $p := (E', F', R')$ deux représentants de degrés de. Le téléphone suivant est appelé *injection virtuelle de n dans p*:

- C'est un téléphone à deux combinés.

- Le clavier du premier combiné est E.
- Le clavier du deuxième combiné est F'.
- L'écran du premier combiné est E'.
- L'écran du deuxième combiné est F.
- La garantie est l'ensemble des $((q,r),(r',q'))$ tels que $(q,q') \in R$ ou $(r,r') \notin R'$

Ce téléphone sera noté (abusivement) $Injvirt(n,p)$, le contexte fournissant la définition adéquate. Il est évidemment bottomludique ssi $n \leq_{Tukey} p$

La question simple suivante prend alors sens: *est-ce que si je dispose de suffisamment de magie pour injecter* 8 *dans* 7*, je peux m'en servir pour injecter* 7 *dans* 6*?* et peut être traduite en la question mathématique: *est-ce que, en notant* $a := Injvirt(7,6)$ *et* $b := Injvirt(8,7)$*, on a* $a \leq_{ludique} b$*?*

Intuitivement, on peut penser que la réponse est oui. En fait, c'est non. Plus précisément on a:

Théorème 91 *Avec la notation précédente, b est ludiquement inférieur à a, mais a n'est pas ludiquement inférieur à b.*

Preuve : Laissée au lecteur

4.2 Droites et paires

On a le sentiment intuitif qu'envoyer une droite D du plan contenant un point (de ce plan) est "beaucoup moins puissant" qu'envoyer une paire de points du plan contenant ce point.

Le théorème suivant nous informe formellement que notre intuition se trompe, mais d'abord :

Définition 92 *On appelle envoidroites le représentant du degré de Tukey (E,F,R) où $E :=$ le plan $\mathbb{R}^2$ et $F :=$ l'ensemble des droites affines de ce plan et $R := \in_{E\times F}$.*

En français, le téléphone de Tukey garantie par *envoidroites* est composé comme suit:

- un clavier dont les touches sont les éléments de $\mathbb{R}^2$
- un écran dont les sorties sont les droites
- Il garantit que si on tape x sur le clavier à l'émission, le récepteur reçoit une droite d telle que $x \in d$

Définition 93 *Soit c un cardinal. On appelle $couv(c,E)$ le représentant du degré de Tukey (E,F,R) où $F :=$ l'ensemble des parties X de E telles que $card(X) \leq c$ et $R := \in_{E\times F}$.*

Il est évident que *envoidroites* $\leq_{Tuk} couv(2,\mathbb{R}^2)$. En fait,

Théorème 94 *envoidroites* $==_{Tuk}$ $couv(2, \mathbb{R}^2)$

On remarque que la preuve utilise une réduction non continue et qu'il ne peut en être autrement!

Preuve : On note $Plan$ l'ensemble $\mathbb{R}^2$. On le suppose muni de sa structure euclidienne canonique et du repère canonique de $\mathbb{R}^2$

Soit j une injection de $Plan$ dans $Cercle$, où $Cercle$ est le cercle unité de $Plan$. On dessine la réduction:

$$x \to j(x) \mid d \to \{t \in Plan \mid j(t) \in d \cap Cercle\}$$

4.3 Généralisation

Dans cette section, on remplace "droite" par "sous-espace affine de dimension n".

Définition 95 *Soit E un espace affine sur $\mathbb{R}$ et n un entier naturel non nul. On appelle $Envoisev(E, n)$ le représentant du degré de Tukey $(E, F, \in_{E\times F})$ où F est l'ensemble des sous-espaces affines de dimension n de E.*

Voici une généralisation du théorème précédent. On notera que la dimension de E peut être petite.

Théorème 96 *Soit E un espace affine sur $\mathbb{R}$. Pour tout entier $n \neq dim(E)$: $couv(n, E) \leq_{Tuk} envoisev(E, n)$*

Remarque : Si $n > dim(E)$ alors $envoisev(E, n)$ est TopTukey car ... F est vide.
Si $n = dim(E)$, alors $F = E$ et $envoisev(E, n)$ est BottomTukey.
On supposera dans ce qui suit que $n < dim(E)$

La démonstration est la même que pour les droites. Il suffit juste de s'assurer que:

Lemme 97 *Soit E un espace affine sur $\mathbb{R}$ de dimension strictement supérieure à l'entier n. Alors il existe une partie A de E avec $card(E) \leq card(A)$ et telle que pour tout sous-espace affine F de E de dimension n, $card(F \cap A) \leq n$*

Preuve : On note Y l'ensemble des sous-espaces vectoriels de E de dimension n. La démonstration utilise l'axiome du choix. Elle reste valable si on remplace $\mathbb{R}$ par un corps K infini. Notons κ le cardinal de $\mathbb{R}$, D l'ensemble des droites engendrées par une base de E et $\delta = card(D)$. Il est facile d'établir que $card(E) = \sup(\kappa, \delta)$. - Si $card(E) = \delta$, on choisit $A = D$. On a $\forall y \in Y$, $card(y \cap A) \leq \dim(y) \leq n$. - Si $card(E) = \kappa$, on considère $B = (e_i)_{0 \leq i \leq n}$ une famille libre de $n+1$ vecteurs de E et C la courbe décrite par le point

$$M_x = \sum_{i=0}^{n} x^i e_i,\ x \in \mathbb{R}^*$$

. L'application $x \to M_x$ est trivialement une bijection de $\mathbb{R}^*$ sur C qui a donc même cardinal que $\mathbb{R}$, puisque ce dernier est infini. On prend alors $A = \{M_x \mid x \in \mathbb{R}^*\}$. On note $G = vect(B)$. Soit $y \in Y$. Il existe un hyperplan H de G contenant $y \cap G$ d'équation $\sum_{i=0}^{n} \alpha_i z_i = 0$, avec un des α_i, $0 \leq i \leq n$ non nul. Notons S l'ensemble des racines du polynome non nul $\sum_{i=0}^{n} \alpha_i x^i$. On a $card(S) \leq n$. Alors $y \cap A \subset \{M_x \mid x \in S\}$ et ce dernier ensemble est de cardinal $\leq n$.

Remarque : Lorsque E est un espace vectoriel de dimension finie sur un corps fini, il nous semble que le résultat tombe en défaut, mais nous n'avons pas approfondi la question.

4.4 Additivité des ultrafiltres

Définition 98 *Soit (E, U, f) tel que U est un ultrafiltre sur E et f une application de E dans F. L'ultrafiltre image de U par f est l'ensemble des parties Y de F telles que $\{x \in E \mid f(x) \in Y\} \in U$.*

On rappelle que l'ultrafiltre image d'un ultrafiltre par une fonction (dont le domaine appartient à l'ultrafiltre) est un ultrafiltre.

Les degrés de Tukey généralisent les cardinaux. L'additivité d'un ultrafiltre est définie par:

Définition 99 *Soit un couple (E, U) tel que U est un ultrafiltre sur E. L'additivité cardinale de U est le plus petit cardinal κ (s'il existe) tel qu'il existe $i \in \kappa \mapsto A_i \in U$ vérifiant $\forall i \in \kappa : A_i \in U$ et $\cap_{i \in \kappa} A_i = \emptyset$*

Remarque : Quand il n'y a pas de confusion redoutée, on abrège en parlant de l'additivité de U.

Par exemple un ultrafiltre qui n'est pas stable par intersections dénombrables a une additivité égale à ω. Un ultrafiltre principal n'a pas d'additivité (entre guillemets, elle dépasse tout cardinal). Un ultrafiltre non principal qui est stable par intersections dénombrables a une additivité au moins égale au plus petit cardinal mesurable.

La notion de cardinal est trop grossière pour saisir, dans le cas particulier des ultrafiltres, la nature profonde de cette additivité, comme on peut le voir avec le saut gigantesque entre ω et le premier cardinal mesurable.

Or ce qu'on attend de l'additivité d'un ultrafiltre est précisément saisi par le degré de Tukey qui lui est rattaché:

Définition 100 *Soit un couple (E, U) tel que U est un ultrafiltre sur E. On désigne par l'expression additivité de Tukey de l'ultrafiltre U, le degré de Tukey dont un représentant est (E, U, R) où $R := \{(x, A) \in E \times U \mid x \notin U\}$. Dans la suite de la section, on notera $add(E, U)$ l'additivité de Tukey de U (sur E)*

On remarque que quand U est principal, l'additivité de Tukey de U est TopTukey. On remarque aussi que U n'a pas besoin d'être un ultrafiltre pour que la définition ait un sens, donc plus généralement:

Définition 101 *Soit un couple (E, U) un couple d'ensembles quelconques. On désigne par l'expression additivité de Tukey du couple (E, U), le degré de Tukey dont un représentant est (E, U, R) où $R := \{(x, A) \in E \times U \mid x \notin A\}$.*

On remarque que l'additivité cardinale de U est le plus petit cardinal κ tel que $add(E, U) \leq_{Tuk} I_\kappa$

Comparons maintenant deux ultrafiltres U, V respectivement sur E, F en terme de Tukey-additivité. On a le résultat suivant :

Lemme 102 *Si $add(E, U) \leq_{Tuk} add(F, V)$ alors il existe une application $f \in (E \to F)$ telle que V est l'image de U par f.*

Preuve : Supposons $add(E,U) \leq_{Tuk} add(F,V)$. Dessinons cette hypothèse:

$$x \in E \to f(x) \in F \mid B \in V \to g(B) \in U$$

dessin qui abrège: pour tout $x \in E, B \in V$ si $f(x) \notin B$ alors $x \notin g(B)$, que l'on peut réécrire en:

$$x \in g(B) \to f(x) \in B$$

. Il s'en suit que l'ultrafiltre V **est l'ultrafiltre image** de l'ultrafiltre U par la fonction f. En effet, soit B un élément de V. Supposons que l'ensemble $A = \{x \in E \mid f(x) \in B$ ne soit pas un élément de U. Alors posons $A := \{x \in E \mid f(x) \notin B\} \in U$ et $A_2 := g(B) \cap A$. On remarque que $A_2 \in U$. C'est une contradiction car $A_2 = \emptyset$. En effet, soit $x \in A_2$. Alors $f(x) \notin B$, donc $x \notin B$ d'après l'hypothèse.

Cela donne un élément de plus illustrant l'intérêt des degrés de Tukey. On s'intéresse à la réciproque:

Preuve : Supposons qu'il existe une application $f \in (E \to F)$ telle que V est l'image de U par f. En posant, pour $g := (B \in V \mapsto \{x \in E \mid f(x) \in B\})$, on obtient le dessin:

$$x \in E \to f(x) \in F \mid B \in V \to g(B) \in U,$$

et on a bien : pour tout $x \in E, B \in V$ si $f(x) \notin B$ alors $x \notin g(B)$

Les argumens précédents donnent le théorème bien connu:

Théorème 103 *Soient (E,U) et (F,V) tels que U est un ultrafiltre sur E et V est un ultrafiltre sur F. Alors $add(E,U) \leq_{Tuk} add(F,V)$ si et seulement si il existe une application $f \in (E \to F)$ telle que V est l'image de U par f*

La définition historique pour $add(E,U) \leq add(F,V)$ est:

Définition 104 *On appelle ordre Rudin Keisler entre les ultrafiltres celui défini par*

$$[(E,U) \leq_{RK} (F,V)] := [add(E,U) \leq_{Tuk} add(F,V)]$$

Inutilité de préciser un support

Un ultrafiltre est un ensemble parmi d'autres. Si U est un ultrafiltre sur E et $E \subseteq F$ alors U induit naturellement l'ultrafiltre image U' de U par $id : E \to F, x \mapsto x$, qui est un ultrafiltre sur F que l'on considère en pratique comme *le même élément fantôme* que U. Ce "évidence intuitive" est en fait soutenue par le théorème suivant:

Théorème 105 *Soit U un ultrafiltre sur E, soit $A \in U$. L'ensemble $V := \{X \subseteq A \mid X \in U\}$ a comme image par $id : A \to E, x \mapsto x$ l'ultrafiltre U.*

Autrement dit, intuitivement, tout ultrafiltre doit être considéré comme un ultrafiltre sur l'univers entier et quand $E \in U$ et X est quelconque, la réponse à la question

X est-il essentiellement un élément de U? La réponse est :

- oui quand $X \cap E \in U$
- non quand $X \cap E \notin U$.

Finalement, soit E un ensemble et U un ultrafiltre sur E, il est évident que:

Théorème 106 *L'additivité de Tukey du couple (E,U) (notée ci-dessus $add(E,U)$) ne "dépend pas" de E, dans le sens que pour toute partie A de E telle que $A \in U$, on a l'égalité au sens de Tukey:*

$$add(E,U) ==_{Tuk} add(A, U \cap P(A))$$

4.5 Deux exemples topologiques

Dans la section précédente, on a associé des degrés de Tukey à des objets. On varie un peu en associant à des objets topologiques un degré ludique, comme il apparaît dans les sous-sections suivantes.

4.5.1 Anticompacité

Intuitivement, quand un espace n'est pas quasicompact, le degré d'anticompacité de cet espace doit être trivial et réciproquement (on mesure la magie à mettre en oeuvre pour l'empêcher d'être quasicompact). Dans la suite, on utilisera le mot *compact*, plus court à écrire, à la place de *quasicompact*

Définition 107 *Soit (E, T) un espace topologique, T étant l'ensemble de ses ouverts. On lui attache un représentant de degré ludique d'uplicité2. On le décrit par la métaphore téléphonique.*

- *Clavier du combiné1* $:= E$
- *Ecran du combiné1* $:= T$
- *Clavier du combiné2* $:=$ *l'ensemble des parties finies F de T telles que union$(F) = E$*
- *Ecran du combiné2* $:= T$
- *La garantie $G :=$ l'ensemble des $((x, U), (F, V))$ tels que $x \in U$ et $V \in F$ et V n'est pas inclus dans U*

Et on note ce représentant anticompact(E, T)

Intuitivement, un espace est plus compact qu'un autre quand son degré d'anticompacité est ludiquement plus grand que celui de l'autre.

Théorème 108 *Les espaces non compacts ont tous un degré d'anticompacité trivial.*

La preuve est évidente

Le choix, hélas (et c'est un point général), d'association à tel ou tel théorème d'un degré ludique qui, entre guillemets, mesure la "magie" à déployer pour aller "contre" sa réalisation peut apparaitre, dans bien des circonstances, un peu arbitraire. Voici un autre exemple:

4.5.2 Anticonnexité

Soit (E, T) un espace topologique et a, b des points de E.

Définition 109 *On appelle disconnect(a, b, E) le degré ludique réprésenté par la garantie du téléphone suivant, d'uplicité2:*

- *Clavier du combiné1* $:= E$
- *Clavier du combiné2* $:= E$
- *Ecran du combiné1* $:= T \times 2$
- *Ecran du combiné2* $:= T \times 2$

- *Garantie* $:=$ *l'ensemble des* $((x,(U,i)),(y,(V,j)))$ *tels que* $U \cap V = \emptyset$ *et* $(x,y) \in U \times V$ *et (si* $(x,y) = (a,b)$ *alors* $i \neq j$*, sinon, si* $y \in U$ *alors* $i = j$*, sinon, si* $x \in V$ *alors* $i = j$*).*

Une fois de plus, avec cet exemple:

Théorème 110 *Si deux points* a, b *d'un espace* (E,T) *n'y sont pas connectés, alors* $disconnect(a,b,E)$ *est un degré ludique trivial et réciproquement.*

4.6 Degré d'information sur l'invisibilité du vivant

La problématique qui émerge des jeux est la suivante: les mathématiques nous enseignent que les jeux à information parfaite de longueur finie à 2 joueurs (2 joueurs au plus comme on l'a vu) sont déterminés. ZF ne supporte pas l'axiome que tous les jeux à information parfaite sont déterminés, ni même que tous les jeux de longueur ω le soient. Il semble par contre supporter l'axiome de détermination et même $AD(\mathbb{R})$. C'est l'axiome d'extensionnalité plus la possibilité de jouer les coups dans de grands ensembles qui conduisent à l'existence de jeux non déterminés. L'axiome du choix contredit aussi $AD(\mathbb{N})$.

Pour, en pratique, trouver des jeux non déterminés on est donc, (on:="êtres humains") obligés de recourir à des limitations physiques (football, tennis), à de l'information cachée (le poker), ... etc ..., mais chaque fois ces informations sont physiquement accessibles **aux arbitres** ou sont matérielles. On peut donc se demander ce qu'il en est quand l'information n'est pas accessible à un arbitre non surhumain et n'est pas matérielle. On ne répond bien sûr pas ici à cette question, mais on mentionne le grand collapse qui se produit pour les jeux usuels à information parfaite. Tous les jeux ici concernés peuvent être formalisés de la manière suivante: un triplet (E,m,P) où m est une application de E^2 dans P. Intuitivement, m est l'opération qui à un couple de stratégies (E étant l'ensemble des stratégies) associe le match qu'elles se livrent.

Soit $z := (E,m,P)$ avec $m \in (E^2 \to P)$ et soit A une partie de P. On note T_z le représentant de Tukey suivant: $T_z := (E, E, \{(x,y) \in E^2 \mid m(x,y) \in A\})$. Intuitivement, c'est le niveau de connaissance pour le joueur2 nécessaire et suffisant **qu'il doit avoir de la stratégie de son adversaire** pour pouvoir le battre. Enoncer la détermination d'une classe de jeux, c'est énoncer que tous les T_z appartiennent à $\{BottomTukey; TopTukey\}$. La question se pose de savoir **en ce qui concerne les jeux à information parfaite** s'il y a beaucoup ou non de degré de Tukey de la forme T_z. La réponse est intéressante. Elle nécessite auparavant un lemme technique: On note S_i l'ensemble des stratégies du joueur i pour chaque $i \in \{0;1\}$

Lemme 111 *Soit* D *une partie dénombrable de* S_0*. Soit* A *un jeu non strat-gagnable par le joueur* 0*. Alors il existe une stratégie* t *dans* S_1 *telle que* $\forall s \in D : t$ *bat* s

Preuve : Ceci est une esquisse de preuve. On trouvera une preuve complète dans [Cha4]. On remplace le jeu A par le jeu A' suivant: une partie p fait gagner le joueur 1 quand non seulement elle le fait gagner au jeu A, mais encore elle doit être telle qu'à n'importe quel moment de la partie, la situation au jeu A pour le joueur 1 ne doit pas être désespérée.

Soit $s_1, s_2, ...$ les éléments de D. Soit p_1 une partie gagnée **au jeu** A' par le joueur 1 et jouée, en tant que joueur 0 par s_1. Regardons la stratégie partielle t_1 suivante: *jouer comme si on était sûr que c'est la partie* p_1 *qui allait se dérouler.* A la moindre rupture avec ce pari, refuser de jouer. Cette stratégie bat s_1 en jouant p_1. Contre s_2, ou bien elle joue p_1, ou bien elle s'arrête de jouer à un moment. C'est forcément à un moment où s_2 vient de rompre la promesse de construire p_1. Dans ce cas, la position des deux joueurs est telle que la situation du joueur 1 n'est pas désespérée au jeu A (par définition de A'). Il existe donc une partie p_2 perdue par s_2 qui est dans A' et qui continue la partie commencée. On continue ainsi le raisonnement jusqu'à avoir construit une suite de parties $(p_1, p_2, ...)$ qui ont la propriété suivante: *il existe une stratégie $t \in S_1$ telle que pour tout entier n : le match que livre t contre s_n est p_n.* Comme toutes ces parties sont dans A', elles sont toutes dans A et t a bien battu toutes les s_n au jeu A.

Théorème 112 *(Hypothèse du continu) Pour tout $z := (E, m, P)$ qui formalise un jeu à information parfaite dont les coups sont des éléments de $\mathbb{R}$, le degré de Tukey de T_z appartient à l'ensemble à trois éléments suivant: $\{TopTukey; BottomTukey; D_{\omega_1}\}$*

Preuve : On peut supposer que le jeu n'est pas déterminé. Soit $<$ un bon ordre sur $S := S_0 \cup S_1$ tel que pour toute $s \in S : \{t \in S \mid t \leq s\}$ est dénombrable (ie $(S, <)$ est isomorphe à $(\omega_1, \in)$). Soit $s \in S_1$. On note $t(s)$ la plus <petite des stratégies $t \in S_0$ telle que $\forall s' \leq s$, t bat s' au jeu A (lemme précédent).

$$s \to t(s) | s' \to s'$$

réduit $D_{\omega_1} := (\omega_1, \omega_1, \in)$ à T_A. On a donc: $\underline{D_{\omega_1} \leq_{Tukey} T_A}$

La symétrie de la situation des joueurs dans le lemme précédent fait que T_A est de la forme $dual(T_{echange(A)})$. L'autodualité de D_{ω_1} entraine donc avec le même raisonnement, appliqué à $echange(A)$, que $\underline{D_{\omega_1} \geq_{Tukey} T_A}$. Conclusion:

$$D_{\omega_1} :==_{Tukey} T_A$$

La question se pose donc de savoir si on a la même rareté des degrés T_z en **l'absence de l'hypothèse du continu**.

4.7 Exemple quantiques

Nous signalons sans démonstration (ils seront disponibles sur HAL) quelques téléphones réellement fabricables par la MQ.

4.7.1 Coloration quantique de la sphère S_3 avec 4 couleurs

- Uplicité 2
- Claviers de chaque combiné: $\mathbb{R}^4$
- Ecrans $4 := \{0; 1; 2; 3\}$
- Garantie: si $u \perp v$ alors $i \neq j$ et si $u = v$ alors $i = j$

La preuve est immédiate en regardant $\mathbb{R}^4$ comme le corps de quaternions: à chaque élément $u \in \mathbb{R}^4$ qui est non nul, on lui associe la base $(u, u \times i, u \times j, u \times k)$. L'objet quantique (le vecteur de $\mathbb{R}^4 \otimes \mathbb{R}^4$) composé de deux parties intriquées peut être ici identifié au produit scalaire usuel

4.7.2 Exemple de R.Penrose

Déjà donné dans l'introduction. Sa non localité est évidente: il n'existe pas matrice 3×3 dont toutes les colonnes contiennent un nombre pair de 0 et toutes les lignes contiennent un nombre impair de 0.

Chapitre 5

Considérations physiques

5.1 Déterminisme vs non déterminisme

Soit (E^2, F^2, G) une garantie téléphonique. Nous prouvons dans ce paragraphe que si G est non triviale alors dès qu'on suppose le déterminisme d'une physique qui offre un téléphone G-garanti on peut se servir de ce téléphone pour violer la relativité. Il s'en suit que toute physique garantissant des degrés ludiques non triviaux est incompatible avec la relativité.

Reformulé de manière vulgarisée, cela peut s'énoncer:

Théorème 113 *Aucune physique qui offre un téléphone G-garanti, où G est non trivial, ne peut à la fois*

- *être compatible avec la relativité ET*
- *être une sous-théorie d'une théorie à variables cachées.*

On suppose dans ce paragraphe qu'on dispose d'un téléphone G-garanti (notons-le T) et que G est non triviale. L'hypothèse déterministe (ou variables cachées éventuellement connues) entraîne l'existence d'un téléphone physiquement fabricable qui est H-garanti avec:

- $H \subseteq G$
- H est le graphe d'une fonction h allant de E^2 dans F^2

Quel est ce téléphone? Réponse: et bien tout simplement T lui-même. En effet, seule la garantie change. Le fait qu'il n'existe pas plusieurs histoires possibles qui racontent les réponses possibles que T offrira aux input est simplement l'expression "en français" que pour tout couple $(x, y) \in E^2$ il existe un unique couple $(r, s) \in F^2$ tel qu'il existe une histoire qui raconte que la réponse que T fournit à l'input (x, y) est (r, s) Or cette condition a une définition mathématique bien connue: elle dit que l'ensemble H des $([x, y], [r, s])$ tel qu'il existe une histoire qui raconte qu'à l'input $[x, y]$ (toute chose égale par ailleurs) le téléphone T répond $[r, s]$ est un graphe de fonction.

L'hypothèse du déterminisme (ou de variables cachées quelles qu'elles soient commandant les réponses de T) entraîne donc que non content d'être G-garanti, T est H-garanti. Le fait que l'on connaisse ou non cet ensemble H n'a aucune importance et le terme "variables cachées" est mal choisi ici en ce qu'il peut conduire à une confusion. Ce terme n'est qu'une invention philosophique verbale dont les philosophes ont le secret...

Le fait que H soit le graphe d'une fonction entraîne que l'on peut considérer H comme l'ensemble des $[x, y], [f(x, y), g(x, y)]$ quand (x, y) parcourt E^2. La non-trivialité de G, donc de H, entraine qu'il n'exite pas de couple (f', g') de fonctions vérifiant: $\forall(x, y) \in E^2 : ([x, y], [f'(x), g'(y)]) \in H$. Par conséquent, quitte à échanger les deux combinés, il existe a, u, v des éléments de E tels que $f(a, u) \neq f(a, v)$; Nous allons en déduire un lien de causalité parfaitement concret qui transmet un bit d'information du combiné2 vers le combiné1.

Appelons Alice l'utilisatrice du combiné2 et Bob l'utilisateur du combiné1. Alice veut transmettre à Bob un bit d'information en utilisant le H-téléphone T. Voici la stratégie:

- Bob tape a sur son clavier.
- Si elle veut transmettre "vert", Alice tape u sur son clavier.
- Si elle veut transmettre "rouge", Alice tape v sur son clavier.
- Si Bob voit apparaître $f(a, u)$ sur son écran alors il sait que Alice lui a dit "vert"
- Si Bob voit apparaître $f(a, v)$ sur son écran alors il sait que Alice lui a dit "rouge"

5.1.1 conclusion

Alice et Bob peuvent se servir de T (qui est un téléphone H-garanti) pour se transmettre un bit d'information dans le sens "de Alice vers Bob".

Théorème 114 *Pour toute uplicité, toute garantie téléphonique qui est un graphe de fonction est ou bien triviale ou bien TSD.*

Ci-dessus, nous avons démontré cet énoncé pour l'uplicité2. La généralisation à l'uplicité quelconque est immédiate.

La conclusion interprétative de ce théorème est que les interprétations "à la Bohm" (variables cachées non locales) de la physique actuelle, dès lors qu'on admet ses postulats à la fois quantiques et relativistes, sont définitivement incompatibles avec la relativité, donc fausses dans le paradigme actuel de la physique qui veut que **les conséquences reproductibles** aussi bien de la mécanique quantique que de la relativité ne seront pas falsifiées par la Nature (par l'expérience).

5.1.2 Remarque

dans la mesure où ce sont là des théorèmes formels concernant des objets finis et que ces théorèmes ne nécessitent aucune hypothèse "philosophique", il y a indiscernabilité linguistique entre "indéterminisme" et "multimondisme".

Précisément, supposons la négation de toutes les interprétations de type "mondes multiples" possibles et imaginables. (Autrement dit, admettons l'idée que nous vivons dans "un seul" monde et que la notion d'indéterminisme s'apparente à "une sélection"(***) parmi des éventualité "physiquement possibles"). Alors, cela revient à admettre "des variables cachées". Quelles sont-elles? Et bien simplement l'ensemble des histoires sélectionnées dans (***)

Par conséquent, l'ensemble P des prédictions concrètes faites par [MQ[1] + relativité] forme une théorie physique qui implique la négation de la conjonction de toutes les négations d'interprétations de type "mondes multiples". Et finalement, il existe au moins une interprétation de type "monde multiple" qui est "la bonne interprétation" de l'ensemble P des prédictions concrètes de [MQ + relativité].

Cette phrase engoncée n'est que la traduction formelle du fait que le mot "indéterminisme" n'est en fait jamais utilisée concrètement dans les preuves d'indétermination de la MQ. A sa place, on trouve des démonstrations de non unicité d'indices, qui sont des non unicités de mondes. On reprend dans la section suivante le même argument, mais en rédigeant plus formellement.

5.2 Indéterminisme prouvable

5.2.1 Introduction

Cette section est consacrée à rendre la section ci-dessus formelle, mais qui prouve “irréfutablement” l'indéterminisme de la Nature dès lors qu'on la suppose soumise aux postulats quantiques ET relativistes et dès lors qu'on suppose une nature “unimonde” de notre univers. Cette section **répète** dans un style plus froid le même argument, afin que le lecteur puisse avoir deux angles

5.2.2 Quand la garantie est un graphe de fonction

Soit T un téléphone ludique d'uplicité2, c'est à dire, de signature $((E_1 \times F_1) \times (E_2 \times F_2), G)$. On note H l'ensemble des $((x_1, x_2), (y_1, y_2))$ tels que $((x_1, y_1), (x_2, y_2)) \in G$.

On s'intéresse à une situation hypothétique que l'on peut exprimer en français par: *la Nature est déterministe.* Cette situation se traduit par (sans interface modélisatrice spéculative): H est un graphe de fonction (ou plus précisément, si on veut être parfaitement précis: G est tel que H est un graphe de fonction)

Théorème 115 *Supposons que T n'est pas trivial et que H est un graphe de fonction. Alors T est TSD*

Preuve : pour $x \in E_1 \times E_2$, on notera l'unique y tel que $(x, y) \in H$ par $(H_1(x), H_2(x))$. Quitte à permuter les indices 1,2, on peut supposer qu'il existe $a \in E_1, b \in E_2, c \in E_2$ tels que $u := H_1(a, b) \neq H_1(a, c) =: v$.

[1] Mécanique Quantique

La suite décrit comment envoyer un I_2 message du combiné2 vers le combiné1.

On considère que Bob est l'utilisateur du combiné2 et Alice l'utilisatrice du combiné1. On impose à Bob d'envoyer à Alice $x \in 2$. Bob applique la stratégie suivante: *if* $x = 0$ *then appuyer sur la touche b else appuyer sur la touche c.*

De son côté, Alice, séparée de Bob, utilise la stratégie suivante: *appuyer sur la touche a. Lire la réponse: r. If* $r = u$ *then dire "j'ai reçu 0" else dire "j'ai reçu 1"*

Il est facile de vérifier que ces deux stratégies permettent à Alice et Bob de simuler dans le sens combiné2 vers combiné1 un I_2-téléphone de Tukey (ie la transmission d'un bit exact d'information)

La conclusion bien connue mais jamais dite formellement de ce lemme simple, dite en français, est la suivante: la Mécanique Quantique (MQ) et l'hypothèse de déterminisme de la Nature entraine la négation de la relativité (dans son principe le plus fondamental: l'inexistence d'un outil causal et déterministe qui envoie un bit causal plus vite que la lumière).

Il y a une remarque importante à rappeler: la vulgarisation et la communication des physiciens présentent généralement la MQ comme ayant été prouvée indéterministe. Il faut faire attention: ce sont là des arguments raisonnables et sérieux, **mais spéculatifs**. Le problème de l'indéterminisme de **la mécanique quantique seule** est **un problème ouvert**. L'argument précédent, sans hypothèse de symétrie ad hoc rajoutée ni relativité, ne conduit pas à la même contradiction.

A notre connaissance, la seule preuve vraiment irréfutable (car formelle) est celle ci-dessus qui dit que **la conjonction d'une prédiction de la MQ ET d'un principe de la relativité ET de l' hypothèse de déterminisme**[2] **de la Nature** est fausse.

5.2.3 Une erreur courante

Une tentation légitime serait d'interpréter les téléphones matériellement fabriqués par la Nature comme, à défaut de les voir comme utilisant une fonction, de les voir comme *utilisant une des fonctions incluses de leur garantie que nous ne pourrions par principe pas connaître.* Ce n'est hélas pas possible à cause du théorème suivant:

Théorème 116 *(informel) La plupart des classes importantes* C *de degrés ludiques sont irrédutibles dans le sens suivant: si une borne inférieure de degrés appartient à* C *alors l'un des degrés appartient à* C*. (Formellement:) il en va ainsi pour* $C \in \{fortementnonTSD; FMQ\}$

En particulier, ce n'est pas parce qu'un téléphone R-garanti est FMQ que la borne inférieure des G_f quand f parcourt l'ensemble des parties de R est lui-même FMQ. Un tel téléphone peut même être excessivement puissant alors même que le premier est assez faible.

[2]Hors mondes multiples, évidemment! Il s'agit précisément de l'énoncé qui interdit à un téléphone offrant une garantie non triviale d'être nonTSD. La démarche de H.Everett et de ses successeurs a défendu une toute autre forme de déterminisme, que l'on n'évoque pas ici, ou plus précisément que l'on évoque sous la forme MQ + relativité + déterminisme implique $card(Mondes) \geq 2$ (la fonction évoquée devenant une multifonction, ie une simple relation)

5.3 Prouvabilité de la non clonabilité

5.3.1 Introduction

Dans cette section, nous prouvons l'impossibilité de cloner les objets quantiques.

Remarque : Ce théorème est connu, mais est généralement présenté intra-modélisation-spéculative, c'est à dire intra-formalisme (en exhibant de manière détaillée le fait que le clonage ne peut être conçu comme une opération linéaire et non de manière reproductible)

La présentation qui suit permet de décrire une expérience où on obtient, quels qu'en soient les résultats, la conclusion suivante: *ou bien un clonage a raté ou bien une prédiction observable de la théorie quantique a été violée*

5.3.2 Téléphonie

Le théorème suivant bien qu'ayant une preuve évidente, est l'outil qui fait tout le travail:

Théorème 117 *Soit T un téléphone ludique à deux combinés dont la garantie n'est pas triviale. Alors* **toute théorie physique qui prévoit sa fabricabilité** *prédit aussi qu'il existe des entités matérielles non clonables.*

Preuve :

notons la signature du téléphone T par $((E_1 \times F_1) \times (E_2 \times F_2), G)$

On suppose qu'on clone son combiné1 en E_1 exemplaires, obtenant une famille $x \in E_1 \mapsto co_1(x)$ et son combiné2 en E_2 exemplaires, obtenant $x \in E_2 \mapsto co_2(x)$.

On tape la touche $x \in E_1$ sur chaque $co_1(x)$ et on note la réponse $f(x)$ qui s'affiche sur son écran. On tape la touche $x \in E_2$ sur chaque $co_2(x)$ et on note la réponse $g(x)$ qui s'affiche sur son écran.

Par hypothèse, il existe un couple $(a, b) \in E_1 \times E_2$ tel que $((a, f(a)), (b, g(b))) \notin G$. On peut donc conclure que le couple de combinés $(co_1(a), co_2(b))$ a échoué à réaliser le téléphone T. Ces clones étaient donc différents des "vrais" combinés de T.

Remarque : On remarque qu'une condition suffisante pour valider ce raisonnement est **l'existence de téléhpones non triviaux garantis**

5.4 Un exemple à trois combinés: GHZ

5.5 Introduction

Cette section est consacrée à la même preuve, mais avec trois combinés "de l'indéterminisme de la Nature" (sous l'hypothèse unimonde), présentée de façon à être self-contained, c'est à dire accessible à un lecteur qui n'a pas lu le reste. Contrairement à ce qui précède, et vu l'objectif de la section, on va utiliser un téléphone à trois combinés et non deux (ça ne change rien, les prédictions de type EPR sont robustes): en effet, à notre connaissance, GHZ est l'exemple le plus pédagogique et le plus simple qui permet ce genre d'exposé.

Cet indéterminisme a été affirmée très vite à la suite des "chocs" pour l'entendement qu'ont représenté les expériences du début du vingtième siècle qui ont donné lieu à la gestation de la théorie quantique. Hélas cette affirmation n'avait pas le statut d'une preuve, mais d'une sorte de *il va de soi que... compte-tenu de...* que partageaient, sans formalité particulière les premiers physiciens confrontés à ces chocs.

Les termes utilisés par exemple *incertitude d'Heisenberg* ne constituaient pas des preuves mais des principes.

En fait, il faut remarquer que la seule preuve irréfutable connue **suppose** les postulats à la fois de la théorie quantique **mais aussi une petite partie de ceux de l'approche relativiste**. La théorie quantique seule ne peut pas prouver (ne peut pas prédire) actuellement l'indéterminisme de la nature.

5.6 Définitions et théorèmes

Rappel: $A \to B$ est l'ensemble des applications de A dans B, ie l'ensemble des $f \subseteq A \times B$ tels que $\forall x \in A \exists ! y \in B : (x,y) \in f$. L'unique y tel que $(x,y) \in f$ est noté $f(x)$. On notera $f * x := (i \mapsto f(i)(x(i)))$ et indifféremment, $a(b)$ peut parfois être noté a_b mais les sens sont égaux.

Dans la suite on note $(F, +, .)$, le corps à deux éléments $Z/2Z$. En fait, on n'aura besoin que de sa structure de groupe. On note E un ensemble (disjoint de F_2) à deux élément $\{vert; rouge\}$.

On s'intéresse à l'ensemble suivant, noté GHZ. $GHZ := \{(x,y) \in E^3 \times F^3 \mid ($ si $x \in \{vert\}^3$ alors $y_0 + y_1 + y_2 = 1)$ et (si $card(\{i \in 3 | x_i = vert\}) = 1$ alors $y_0 + y_1 + y_2 = 0)\}$.

Le théorème suivant est extrêmement significatif bien que trivial

Théorème 118 *Il n'existe aucun triplet d'applications $(f_0, f_1, f_2) \in (E \to F)^3$ tel que (*) pour tout $x \in E^3 : (x, (i \in 3 \mapsto f_i(x_i))) \in GHZ$*

Preuve :

notons provisoirement $x_i := f_i(vert)$ et $a_i := f_i(rouge)$. Supposons que (f_0, f_1, f_2) vérifie (*). Alors $x_0 + x_1 + x_2 = 1$ et $a_0 + a_1 + x_2 = 0$ et $a_0 + x_1 + a_2 = 0$ et $x_0 + a_1 + a_2 = 0$. Ce qui est contradictoire puisque $x_0 + x_1 + x_2 = 1$ et $a_0 + a_1 + x_2 + a_0 + x_1 + a_2 + x_0 + a_1 + a_2 = x_0 + x_1 + x_2$

Dans le théorème suivant, nous exprimons que si H est un graphe de fonction inclus dans GHZ alors il existe un moyen d'utiliser *le téléphone GHZ* pour transmettre instantanément **un bit** d'information. Le théorème est énoncé dans sa version générale, pour éviter des confusions cabalistiques inutiles.

Théorème 119 *Soient $i \in J \mapsto (E_i, F_i)$ une famille de couples d'ensembles, $(U, V) := (\prod_{i \in J} E_i, \prod_{i \in J} F_i$ et $G \subseteq U \times V$ un graphe de fonction. Supposons qu'il n'existe pas de $f := (i \in J \mapsto (f_i \in E_i \to F_i))$ tel que pour tout $x \in U : (x, f * x) \in G$. Alors il existe $i_0 \in J$, $a \in E_i$, ϕ une fonction de domaine 2 et $\psi \in F_i \to 2$ tel que pour tout $(e, x, y) \in 2 \times U \times V$: si $x_i = a$ et $(i \in J \setminus \{i_0\} \mapsto x_i) = \phi(e)$ alors $\psi(y_{i_0}) = e$*

Preuve : C'est évident.

En français, dans le cas particulier du téléphone GHZ, le théorème dit que si on remplace la garantie GHZ par un graphe de fonction alors il existe un des trois combinés qui peut être pris pour récepteur R, les autres combinés pouvant être regroupés et servir d'émetteur E. On peut alors l'utiliser pour envoyer un élément de 2, c'est à dire un “0” ou un “1” à notre guise en l'émettant sur E. Le récepteur le reçoit sur R, en tapant la touche a sur son clavier.

5.7 Garantie prédite par la Mécanique Quantique (MQ)

Dans cette section, nous précisons la spécification concrète du téléphone GHZ. La théorie quantique **prédit** la possibilité de construire matériellement un appareil qui offre **la garantie** suivante:

- Cet appareil est composé de trois combinés. Aucun fil ne les relie et on peut les emmener où on veut. Il est à usage unique: il s'autodétruit dès qu'il est utilisé
- Chaque combiné a un clavier et un écran
- Le clavier est composé de touches qui sont les éléments de E
- L'écran est un écran “à un seul pixel”, dont la couleur est un élément de F
- Quelle que soit la date (ultérieure à la fabrication du téléphone évidemment) où l'utiliseur appuie sur une touche, dans l'instant qui suit, l'écran affichera une couleur
- les couples $((i \mapsto x_i), (i \mapsto y_i))$ où x_i est la touche appuyée par l'utilisateur i sur son clavier de combiné$_i$ vérifient $(x, y) \in GHZ$.

5.8 Conclusion

Le premier théorème assure que le téléphone (affirmé constructible matériellement par la théorie quantique) GHZ vérifie l'hypothèse du deuxième théorème (il ne réagit pas à ses input comme un graphe de fonction ou alors cette fonction n'est pas locale). Le deuxième théorème assure que si le téléphone répond de manière déterministe (pas forcément locale, juste déterministe) alors il falsifie la relativité dans son extrait *il n'y a pas de possibilité de transmettre un bit d'information à vitesse supérieure à la lumière (ou de causalité à vitesse supérieure à la lumière)*. De manière concrète:

quel que soit l'élément de $E^3 \to F^3$ que Alice propose à Bob pour prétendre lui décrire le comportement (même une seule fois) du téléphone GHZ, Bob peut alors appuyer un triplet de boutons bien choisi sur les écrans de chaque combiné pour invalider la prétention d'Alice ou violer la relativité de manière effective (falsification). **Attention:** il ne s'agit pas ici d'une falsification de variables cachées locales, mais de variables cachées tout court. La vulgarisation a transmis l'idée, fausse, que les intrications quantiques entraient en contradiction avec quelque postulats de variables cachées **locales** que ce soit. On est ici dans un contexte où la vulgarisation s'est fixée sur une position trop modérée. En aucune manière la localité n'est une hypothèse nécessaire pour obtenir une contradiction. Certains évoquent la non possible connaissance des variables cachées globales évoquées ci-dessus pour les déclarer non falsifiable. Les théorèmes qui précèdent ne les supposent pas "connues". Cette notion de "connaissance" n'a d'ailleurs pas de sens ici. Le théorème est de la forme *tout graphe de fonction est incompatible avec ....* Bien évidemment, mais cela n'est pas spécifique à la physique, lorsqu'on prouve $\forall x \exists y R(x, y)$, on ne prouve pas forcément $\exists y \forall x R(x, y)$. Evoquer la non possibilté de connaissance de x pour répondre qu'on ne saurait pas, sans cette connaissance, lui associer le y tel que n'est pas recevable ici. L'énoncé dit que pour tout x, il existe un y qui "falsifie x". Bien évidemment, le y dépend de x.

Chapitre 6

Eternité

6.1 Introduction

On utilise parfois la syntaxe du langage CAML pour certaines définitions. Dans ce chapitre, on tente de comprendre ce que les degrés de Tukey ont à nous dire dans le cadre des questions d'éternité que nous allons aborder. Quels téléphones assurent que leur utilisation répétée garantit pour "le monde" un acte de naissance de principe à une distance temporelle finie dans le passé? On a déjà évoqué que quand on souhaite rajouter des hypothèses de continuité, les espaces topologiques compacts, entre autres, supportent l'éternité.

6.2 Protocoles fictifs

Soit E un ensemble tel que $\mathbb{N} \subseteq E$. Il n'existe pas de suite $u \in E^{\mathbb{N}}$ telle que pour tout entier n:

$$u_n = [\ if\ u_{n+1} \notin \mathbb{N}\ then\ 0\ else\ u_{n+1} + 1]$$

Autrement dit, la possibilité d'accès à une haute résolution de $\mathbb{N}$ (ou plus précisément de $I_{\mathbb{N}}$) garantit à une civilisation que ou bien elle n'existe pas depuis toujours ou bien elle n'applique pas la "mission" suivante depuis toujours: *Chaque jour, à 15H, le gardien de la Boite doit l'ouvrir et la renouveler de la façon suivante: il l'ouvre, regarde l'élément x qu'elle contient, s'il constate que $x \notin \mathbb{N}$, il remplace ce x par 0, sinon, il remplace ce x par $x+1$, puis referme la boite jusqu'au lendemain et veille à ce que personne n'y accède*

La question se pose alors des résolutions à partir desquelles on peut tirer la même conclusion que ci-dessus (en supposant l'immortalité des habitants de la société)

Un théorème ancien, mais fameux[1], affirme qu'un ensemble fini a une trop basse résolution pour permettre un protocole interdisant l'éternité passée d'une civilisation, ce qui formellement s'exprime par:

Théorème 120 *Soit F un ensemble fini et $n \mapsto f_n$ une suite d'applications de F dans F. Alors il existe une suite $u \in F^{\mathbb{N}}$ telle que pour tout $n \in \mathbb{N} : u_n = f_n(u_{n+1})$*

[1]c'est le lemme de König "Tout arbre infini à branchement fini a une branche infinie"

Une approche plus spéculative, qui consiste à faire intervenir des postulats de continuité, est aussi confrontée à un théorème qui dit que la compacité de l'espace ambiant offre une trop faible résolution pour un protocole garantissant un acte de naissance à une civilisation

Théorème 121 *Soit F un ensemble muni d'une topologie compacte et $n \mapsto f_n$ une suite d'applications* **continues** *de F dans F. Alors il existe une suite $u \in F^{\mathbb{N}}$ telle que pour tout $n \in \mathbb{N} : u_n = f_n(u_{n+1})$*

Preuve : C'est une conséquence immédiate du théorème de Tychonov

Remarque : Notons que le résultat tombe en défaut si la topolgie n'est pas séparée. Prendre $F = \mathbb{R}$ muni de la topologie cofinale et $f_n = x \mapsto x + 1$

.

On peut s'étonner du choix conventionnel qui nous a conduit, ci-dessus, à ne permettre au gardien de ne retenir du passé que ce qui a été enregistré la veille. N'est-ce pas contraire à notre expérience? On peut donc formaliser autrement (et de manière non équivalente) la problématique d'une *civilisation qui agit en fonction du passé*

Mais dès lors qu'on autorise la civilisation, non pas à remplir “la Boite” avec un élément pouvant varier dans un gros ensemble, mais, indépendamment de ce remplissage, à se rappeler **tout le passé**, alors ce n'est plus $\mathbb{N}$ qui est un trop gros cardinal mais 2:

Théorème 122 *Soit E un ensemble de cardinal au moins 2. Il existe une application $f : E^{\mathbb{N}} \to E$ telle que pour toute suite $u \in E^{\mathbb{N}}$, il existe un entier n tel que $u_n \neq f(p \mapsto u_{n+p+1})$*

Et en aucune façon l'axiome du choix n'est nécessaire à ce raisonnement:

Preuve : Il est facile de voir que, pour toute suite $u \in 2^{\mathbb{N}}$, il existe $n \in \mathbb{N}$ tel que

$$u_n \neq [\ if\ \exists p > n : u_p = 1\ then\ 0\ else\ 1]$$

L'axiome du choix permet d'aller beaucoup plus loin , puisqu'il permet d'avoir une fonction de Galvin sur n'importe quel ensemble E, On rappelle ce qu'est une fonction de Galvin. On définit pour cela la fonction $S : E^{\mathbb{N}} \to E^{\mathbb{N}}$ (shift gauche) qui, à la suite u associe la suite $S(u)$, définie par la formule: $\forall n \in \mathbb{N},\ S(u)_n = u_{n+1}$

Définition 123 *Soit E un ensemble. On dit qu'une fonction ϕ est une fonction de Galvin sur E si elle est une application de $E^{\mathbb{N}}$ dans E telle que pour toute suite $u \in E^{\mathbb{N}}$, il existe un entier p tel que: $\forall n > p;\ \phi(S^{n+1}(u)) = u_n$*

On rappelle le théorème de Galvin :

Théorème 124 *(Axiome du choix supposé) Pour tout ensemble E, il existe une fonction ϕ de Galvin sur E*

Preuve : voir le chapitre 9 ou [G.P.].

6.3 Définitions formelles et sommaire des théorèmes concernant l'éternité

On rappelle que D_k désigne le triplet $(k, k, \in)$, où k désigne un cardinal infini régulier.

6.3.1 Suites et Degrés éternels

Définition 125 *Soit, pour chaque entier n : (E_n, F_n, R_n) tels que $R_n \subseteq E_n \times F_n$, un représentant de Tukey. On dira que* **cette suite** *est éternelle si: Pour toute suite de fonctions $f_n : F_{n+1} \to E_n$, il existe une suite de $u \in \prod_n E_n$ et une suite de $v \in \prod_n F_n$ telles que pour tout entier n : $f_n(v_{n+1}) = u_n$ et $(u_n, v_n) \in R_n$.*

On dira qu'un triplet (E, F, R) est éternel quand la suite constante $n \mapsto (E_n := E, F_n := F, R_n := R)$ est une suite éternelle.

Les théorèmes établis dans la suite sont les suivants:

- (E, F, R) n'est pas éternel si et seulement si il existe un cardinal régulier et infini k tel que $D_k \leq_{Tukey} (E, F, R)$.
- Une famille quelconque de triplets éternels (E_i, F_i, R_i) est telle que sa borne supérieure est éternelle
- Si une suite de triplets (E_n, F_n, R_n) n'est pas éternelle alors ou bien il existe un entier n tel que le triplet (E_n, F_n, R_n) est TopTukey ou bien il existe un entier n tel que pour tout entier $p \geq n$, le triplet (E_p, F_p, R_p) est non-éternel.
- si (E, F, R) est éternel vu dans un univers V, il est encore éternel vu dans un sous-univers
- il existe un triplet éternel $a := (E, F, R)$ des univers V_1, V_2 tels que a est éternel vu dans V_1 et a ne l'est plus dans V_2 et V_2 est une extension générique de V_1

6.4 Enoncés et preuves détaillées

6.4.1 Définition

Soit $R \subseteq E^2$. Soit deux suites f, g d'applications f_n, g_n de E dans E. On se pose la question suivante:

Est-il possible, avec le R-téléphone, de se garantir qu'on ne peut recevoir un message provenant du passé éternel en même temps qu'on contrôle chaque transmission du jour au lendemain (en choisissant les f_n, g_n comme stratégies)?

Si la réponse est non pour le choix de f, g alors il existe des suites u, v d'éléments de E vérifiant:

1. pour chaque entier n, $f_{n+1}(u_{n+1})Rv_n$ (l'utilisateur du $n+1$ ième composant voit u_{n+1} et envoie un R-message à l'utilisateur n, qui reçoit v_n)
2. pour chaque entier n, $u_n = g_n(v_n)$ (L'utilisateur du n-ième composant crée le u_n en fonction du v_n reçu).

Définition 126 *La conjonction des deux conditions précédentes sera notée* $Eter(R, f, g, u, v)$. *La relation* (R, E) *est dite éternelle quand pour tout couple* f, g *il existe un couple de suites* u, v *vérifiant* $Eter(R, f, g, u, v)$

6.4.2 Robustesse de la notion

Nous allons voir que la notion d'éternité d'un degré de Tukey a des propriétés comme on en trouve rarement en maths. Les voici, de manière répétée, résumées plus informellement:

- Une borne supérieure de degrés éternels est un degré éternel
- S'il n'existe pas de suite u vérifiant $\forall n : u_{n+1}R_n u_n$ alors ou bien l'une des R_n est trivialement TopTukey ou bien **PRESQUE TOUTES**(i.e. toutes sauf un nombre fini) les relations R_n sont non éternelles.
- Ce qui est frappant dans l'item précédent est que les R_n n'ont à priori rien à voir les unes avec les autres et pourtant la conclusion les concerne presque toutes

Lemme 127 (E, E, R) *est éternelle si et seulement si pour toute suite de* $f_n \in (E \to E)$, *il existe une suite d'éléments* $u_n \in E$ *telle que* $\forall n \in \mathbb{N} : (f_n(u_{n+1}), u_n) \in R$.

Pour des raisons similaires,

Lemme 128 *La propriété d'éternité ne dépend que du degré de Tukey de* (E, E, R)

Le théorème principal de ce chapitre est le suivant:

Théorème 129 (E, F, R) *est éternelle si et seulement si il n'existe pas de cardinal régulier* κ *tel que* $D_\kappa \leq_{Tukey} (E, F, R)$

Preuve : Sans perte de généralité on suppose $E = F$. Supposons que (E, E, R) ne soit pas éternelle. Soit des $f_n \in (E \to E)$ qui en témoignent. Pour toute suite $u \in E^{\mathbb{N}}$ il existe un entier n tel que $(f_n(u_{n+1}), u_n) \notin R$.

Notons $T := T(n \mapsto f_n)$ l'ensemble des suites finies $u := (u_0, .., u_n)$ vérifiant $\forall i \in n : (f_i(u_{i+1}), u_i) \in R$. Alors T est un arbre bien fondé. On regarde l'application canonique ϕ_T de T dans l'ordinal attaché κ (qui est la hauteur de l'arbre T) telle que pour tout $(u, v) \in T^2$ si u est un prolongement strict de v alors $\phi_T(v) > \phi_T(u)$.

ϕ_T est définie par $\phi_T(u) :=$ le plus petit ordinal strictement supérieur à tous les $\phi_T(v)$ quand v parcourt l'ensemble $v \in T$ telles que v prolonge strictement u.

Dans la suite, la suite finie u est notée $[u(0); ...; u(n)]$ et si elle est de longueur 1, de seul terme x, elle est notée $[x]$. On peut supposer que R n'est pas de degré $TopTukey$.

On peut supposer qu'on a choisi un contre-exemple (E, E, R) tel que κ soit le plus petit ordinal possible obtensible avec ces propriétés en provenance d'un contre-exemple

Soit $i < \kappa$. L'ordinal i n'est pas attachable à un contre-exemple. Il s'ensuit que la hauteur de l'arbre $T' := T(n \mapsto f_{n+1})$ est au moins égale à κ et donc il existe $x(i) \in E$ tel que $\phi_{T'}([x(i)]) = i$.

Mais alors si $(f_0(x(i)), y) \in R$, il s'ensuit que $\phi_T([y]) > i$ et on vient de réduire D_κ à R.

Il reste à démontrer que κ est un ordinal limite.

Si $\kappa = \mu + 1$ alors il existe $x \in E$ tel que $\phi_{T'}([x]) = \mu$. Comme R n'est pas $TopTukey$, il existe $y \in E$ tel que $(f_0(x), y) \in R$. OR cela entraine que $\phi_T([y]) \geq \kappa$ et c'est une contradiction.

6.5 Stabilité de l'éternité

Dans cette section nous allons voir qu'une borne supérieure de degrés éternels est éternelle. Soit k un cardinal infini et régulier.

6.5.1 Degrés irréductibles

Théorème 130 *Soit k un cardinal infini régulier et $j \in J \mapsto v_j := (E, E, R_j)$ une famille telle que D_k soit "Tukey inférieure" à la borne supérieure s des $v_j, j \in J$. Alors il existe $i \in J : D_k \leq_{Tukey} v_i$*

Preuve : Il existe une stratégie de réduction

$$\alpha \to (i(\alpha), x(\alpha)) | f \to \phi(f)$$

de D_k à s, ce qui signifie que pour tout $\alpha; f$: si $(x(\alpha), f(i(\alpha))) \in R_{i(\alpha)}$ alors $\alpha < \phi(f)$.

Comme k est régulier, on se trouve devant l'alternative:

- Il existe $j \in J$ et une partie non bornée A de k telle que $\forall \alpha \in A : i(\alpha) = j$. Dans ce cas $D_k \leq (E, E, R_j)$ comme attesté par la stratégie $\alpha \in A \to x(\alpha)|y \to \phi(Constante(y))$, qui peut être légèrement modifiée pour remplacer A par k tout entier.
- Il existe une partie non bornée A de k telle que la restriction de i à A est injective. Dans ce cas, il existe une fonction f vérifiant $\forall \alpha \in A : (x(\alpha), f(i(\alpha))) \in R_{i(\alpha)}$ et il s'ensuit que $\phi(f)$ est majorant de A dans k ce qui est une contradiction.

Définition 131 *Soit d un degré de Tukey. Il est dit irréductible quand pour toute famille $(a_i)_{i \in J}$ de degrés vérifiant $sup_i a_i \geq d$, il existe $j \in J : a_j \geq d$.*

Le théorème précédent dit que tous les D_k sont irréductibles, dès lors que k est un cardinal régulier infini.

Il y a d'autres degrés irréductibles, en l'occurence tous les duaux des I_n quand n est un entier. En effet:

Théorème 132 *Soit $(v_i, i \in I)$ une famille de relations de Tukey, n un ensemble quelconque et on suppose que $\inf_{i \in I} v_i \leq I_n$. Alors il existe un indice i tel que $v_i \leq I_n$.*

Preuve : Regardons une réduction de la forme $f \mapsto k(f) \in I_n | p \in I_n \mapsto (i(p), y(p))$ qui garantit que si $k(f) = p$ alors $(f(i(p)), y(p)) \in R_{i(p)}$.

Le lemme de l'étoile assure l'existence d'un indice j et d'une famille $x \mapsto f_x$ vérifiant $i(k(f_x)) = j$ et $f_x(j) = x$ pour tout x. Soit $g : x \mapsto k(f_x)$. Alors

$$x \mapsto g(x) \in I_n \mid p \in I_n \mapsto y(p)$$

réduit v_j à I_n du fait que si $p = g(x)$ alors $p = k(f_x)$, donc $(x = f_x(j) = f_x(i(p)), y(p))$ est un élément de R_j car ce R_j est $R_{i(k(f_x))}$.

Analogie avec une célèbre conjecture, celle de Hedetniémi

Un corollaire de ce théorème est que si T_G, T_H sont les degrés de Tukey associés aux graphes G, H, et si ni G ni H ne sont coloriables avec n couleurs alors le degrés de Tukey $inf(T_G, T_H)$ n'est pas réductible à I_n. Un conjecture célèbre dit, en contraste avec ce résultat que:

Question 133 *Pour tous graphes G, H et tout entier n, si ni G ni H ne peuvent être coloriés avec n couleurs alors le produit $G \otimes H$ non plus?*

Cette conjecture **est la conjecture de Hedetniemi**

Remarque : Evidemment, $T_{G \otimes H} \leq inf(T_G, T_H)$. Mais rien n'assure que $T_{G \otimes H} \geq inf(T_G, T_H)$

Retour aux degrés éternels

Voici un théorème sur les degrés éternels qui a un profil étonnant:

Théorème 134 *Soit $n \in \mathbb{N} \mapsto (E, E, R_n)$ une suite de relation vérifiant: il n'existe pas de suite $u \in E^{\mathbb{N}}$ telle que*

$$\forall n \in \mathbb{N} : (u(n+1), u(n)) \in R_n$$

On suppose qu'aucune des (E, E, R_n) n'est TopTukey. Alors il existe un entier p tel que pour tout $n \geq p$: R_n est **non-éternelle**

Preuve : S'il existe une infinité d'entiers n tels que R_n est éternelle, comme aucune des R_p n'est TopTukey, on peut remplacer les enchainements de relations non éternelles successives par un graphe de fonction.

Il suffit donc de prouver l'énoncé suivant:

Lemme 135 *S'il n'existe pas de suites u telle que $\forall n \in \mathbb{N} : (f_n(u(n+1)), u(n)) \in R_n$ (***) alors au moins une des R_n n'est pas éternelle.*

Preuve : Soit (F, F, S) une relation Tukey-équivalente à la borne supérieure des $(E, E, R_n), n \in \mathbb{N}$. Chacune des (E, E, R_n) se réduit à (F, F, S) via une stratégie de la forme $e \to g_n(e)|z \to h_n(z)$.

Pour obtenir une suite u qui vérifie (***), on dessine un petit schéma qui aide à comprendre, pour $n := 4$:

$$u_5 \to f_4(u_5) \to_S v_5 := g_4(f_4(u_5))|v_4 \to h_4(v_4) =: u_4$$

assurera que $(f_4(u_5), u_4) \in R_4$.

Il s'ensuit qu'il n'existe pas de suites v vérifiant pour tout entier n:

$$(g_n(f_n(h_n(v(n+1)))), v_n) \in S$$

et donc que S n'est pas éternelle. Par conséquent, il existe un cardinal régulier k tel que $D_k \leq (F, F, S)$.

Or d'après l'irréductibilité de D_k, il existe un entier n tel que $D_k \leq R_n$, ce qui prouve que R_n n'est pas éternelle, CQFD

6.5.2 Application aux théorèmes de la cible

Dans cette sous-section, on décrit le lien entre la propriété d'éternité et les jeux mis en oeuvre dans les phénomènes de Target's dont on rappelle les énoncés, les preuves pouvant être consultées sur HAL[2]. A la fin de cette sous-section, on mentionne à quel point (c'est beaucoup plus visible et important dans les preuves elles-mêmes que dans les énoncés) le fait de remplacer la prise du complémentaire par le dual au sens de Tukey a enrichi l'émergence des cibles concernées (Insoupçonnables quand on regarde $E^2 \setminus A$ au lieu de $E \setminus \{(x, y) \in E^2 \mid (y, x) \notin A\}$).

Deux joueurs, Léa et Bob s'affrontent dans divers jeux à information parfaite de longueur ω, que nous abrégeons de la manière suivante, où E désigne un ensemble quelconque, F aussi et où $\leq$ est un ordre total sur F et ϕ, ψ sont des applications de E dans F.

[2]Voir [Cha2] et [Cha4]

Le jeu $G(E, F, \leq, n, \phi, \psi)$

Léa joue $x_0 \in E$, puis Bob joue $y_0 \in E$, puis Léa joue x_1 puis Bob joue y_1, etc. A chaque étape Léa joue x_i avant que Bob joue y_i **à l'exception de l'étape** n. A l'étape n, Léa joue une relation R incluse dans E^2 **telle que** (E, E, R) **n'est pas un représentant de degré de Tukey éternel**. Bob choisit alors un couple $(x_n, y_n) \in E^2 \setminus R$. C'est ainsi qu'à l'étape n, les deux joueurs construisent leur couple (x_n, y_n).

Le jeu $H(E, F, \leq \phi, \psi, A)$

Léa joue $x_0 \in E$, puis Bob joue $y_0 \in E$, puis Léa joue x_1 puis Bob joue y_1, etc. A chaque étape Léa joue x_i avant que Bob joue y_i

Condition de gain

Dans le jeu $G(E, F, \leq, n, \phi, \psi, A)$, Léa est déclarée gagnante quand $\phi(x) > \psi(y)$. Dans le jeu $H(E, F, \leq \phi, \psi, A)$, Léa est déclarée gagnante quand $\phi(x) > \psi(y)$ ou $\phi(x) = \psi(y) \in A$.

6.5.3 Théorèmes de la cible avec option d'obligation d'éternité lors d'un coup

Théorème 136 *On suppose que $\leq$ est un bon ordre sur F et que les jeux mis en oeuvre sont tous déterminés. Soit T un ensemble non vide inclus dans $F^{E^{\mathbb{N}}}$. Il existe $\phi \in T$ tel que:*

ou bien, il existe **un unique entier** *n tel que pour tout $\psi \in T$: Léa a une stratégie infaillible à $G(E, F, \leq, n, \phi, \psi)$*

ou bien, pour tout $\psi \in T$: l'ensemble des parties A de F telles que Léa a une stratégie infaillible pour gagner $H(E, F, \leq \phi, \psi, A)$ est un ultrafiltre sur F stable par intersections dénombrables. En particulier, si F est dénombrable alors cet ultrafiltre est principal et l'élément, unique, de F qui est concerné s'appelle le target de T.

Les deux conclusions s'excluent l'une l'autre. Dans le cas particulier où E est muni d'une topologie (on met sur $E^{\mathbb{N}}$ la topologie produit) qui le rend compact et où $T = \{\phi\}$ avec ϕ continue $E^{\mathbb{N}}$ dans F, si le premier cas n'est pas satisfait alors il existe $x \in E^{\mathbb{N}}$ tel que pour tout $y \in E^{\mathbb{N}} : \phi(x) \geq \phi(y)$

Le deuxième théorème de la cible fournit les mêmes conclusions, mais la seule hypothèse faite sur l'ordre est qu'il est un ordre total (il n'est plus supposé qu'il est un bon ordre).

Théorème 137 *On suppose que $\leq$ est un bon total sur F et que les jeux mis en oeuvre sont tous déterminés. Soit ϕ un élément de $F^{E^{\mathbb{N}}}$.*

ou bien, il existe **un unique entier** *n tel que Léa a une stratégie infaillible à $G(E, F, \leq, n, \phi, \phi)$*

ou bien, l'ensemble des parties A de F telles que Léa a une stratégie infaillible pour gagner $H(E, F, \leq \phi, \phi, A)$ est un ultrafiltre sur F stable par intersections dénombrables. En particulier, si F est dénombrable ou égal à $\mathbb{R}$ alors cet ultrafiltre est principal et l'élément, unique, de F, qui est concerné s'appelle le target de ϕ.

Les deux conclusions s'excluent l'une l'autre.

Le troisième théorème de la cible est une version min-max qui généralise la notion de détermination (on y retrouve la propriété générale de détermination en se plaçant dans l'ensemble totalement ordonné canonique à deux éléments). La description des jeux y est un peu différente.

Le jeu $GG(E, F, \leq, n, \phi)$

Léa joue x_0. Bob joue y_0. Puis Léa joue y'_0, puis Bob joue x'_0. Léa joue x_1. Bob joue y_1. Puis Léa joue y'_1, puis Bob joue x'_1. Et ainsi de suite. A l'étape exceptionnelle n, Léa joue une relation R incluse dans E^2 **telle que** (E, E, R) **n'est pas un représentant de degré de Tukey éternel**. Bob choisit alors un couple $(x_n, y_n) \in E^2 \setminus R$. Puis Léa joue y'_n, puis Bob joue x'_n. Les deux joueurs construisent ainsi chacun un élément de $(E^{\mathbb{N}})^2$.

Le jeu $HH(E, F, \leq, \phi)$

Léa joue x_0. Bob joue y_0. Puis Léa joue y'_0, puis Bob joue x'_0. Léa joue x_1. Bob joue y_1. Puis Léa joue y'_1, puis Bob joue x'_1. Et ainsi de suite. Il n'y a pas d'étape exceptionnelle. Les deux joueurs construisent ainsi chacun un élément de $(E^{\mathbb{N}})^2$.

Condition de gain

Dans le jeu $G(E, F, \leq, n, \phi, \psi, A)$, Léa est déclarée gagnante quand $\phi(x, x') > \psi(y, y')$. Dans le jeu $H(E, F, \leq \phi, \psi, A)$, Léa est déclarée gagnante quand $\phi(x, x') > \psi(y, y')$ ou $\phi(x, x') = \psi(y, y') \in A$.

6.5.4 Théorèmes min-max de la cible

Théorème 138 *On suppose que $\leq$ est un bon ordre sur F et que les jeux mis en oeuvre sont tous déterminés. Soit T un ensemble non vide inclus dans $F^{(E^{\mathbb{N}})^2}$. Il existe $\phi \in T$ tel que:*

ou bien, il existe **un unique entier** *n tel que pour tout $\psi \in T$: Léa a une stratégie infaillible à $GG(E, F, \leq, n, \phi, \psi)$*

ou bien, pour tout $\psi \in T$: l'ensemble des parties A de F telles que Léa a une stratégie infaillible pour gagner $HH(E, F, \leq \phi, \psi, A)$ est un ultrafiltre sur F stable par intersections dénombrables. En particulier, si F est dénombrable alors cet ultrafiltre est principal et l'élément, unique, de F qui est concerné s'appelle le target de T.

Les deux conclusions s'excluent l'une l'autre.

Le deuxième théorème de la cible affirme les mêmes conclusions, mais la seule hypothèse faite sur l'ordre est qu'il est un ordre total (il n'est plus supposé qu'il est un bon ordre).

Théorème 139 *On suppose que $\leq$ est un bon total sur F et que les jeux mis en oeuvre sont tous déterminés. Soit ϕ un élément de $F^{(E^{\mathbb{N}})^2}$.*

ou bien, il existe **un unique entier** *n tel que Léa a une stratégie infaillible à $G(E, F, \leq, n, \phi, \phi)$*

ou bien, l'ensemble des parties A de F telles que Léa a une stratégie infaillible pour gagner $H(E, F, \leq \phi, \phi, A)$ est un ultrafiltre sur F stable par intersections dénombrables. En particulier, si F est dénombrable ou égal à $\mathbb{R}$ alors cet ultrafiltre est principal et l'élément, unique, de F, qui est concerné s'appelle le target de ϕ.

Les deux conclusions s'excluent l'une l'autre.

6.5.5 Remarques

La détermination de suffisamment de jeux limitent donc, entre autre, fortement les ordres totaux sur l'ensemble $\mathbb{R}$. L'émergence de filtres (qui deviennent des ultrafiltres "proportionnellement" à la détermination des jeux mis en oeuvre) est due au phénomène abstrait algébrique suivant:

Théorème 140 *Soit S une partie de $P(E^2)$ telle que pour tout $A \subseteq E^2 : A \in S$ ou $\{(x,y) \in E^2 \mid (y,x) \notin A\} \in S$. On suppose de plus que pour tout F, G dans S : $F \circ G \in S$ (autrement dit S est stable par composition). Soit $\leq$ un ordre total sur E. Alors l'ensemble des parties X de E tel que $\{(x,y \mid x < y$ ou $x = y \in X)\} \in S$ engendre un ultrafiltre sur E (éventuellement égal à $P(P(E))$). Cet ultrafiltre est stable par intersections dénombrables dès que l'ordre est un bon ordre.*

On note qu'on a "retourné" la négation, ie la condition sur S **n'est pas** "$A \in S$ ou $non(A) \in S$" mais $A \in S$ ou $DualTukey(A) \in S$

6.6 Quand le retournement est inoffensif

Il existe au moins une situation célèbre où la "bonne fondation" dans un sens implique **la bonne fondation dans l'autre sens**. Quand les propriétés structurelles étudiées provoquent cet effondrement de la distinction on peut s'estimer très loin de ordinaux (ils sont l'archétype d'exemple où on peut aller aussi haut qu'on veut dans un sens alors qu'on ne peut descendre qu'un nombre fini de fois dans l'autre sens)

Cette *situation célèbre* est le théorème suivant: *tout anneau commutatif unitaire qui est artinien est aussi noethérien.*

Que se passe-t-il? Pourquoi la structure annelée, ajoutée à la commutativité effacent-elles les émergences précédentes? Pourquoi est-elle assymétrique (certains anneaux noéthériens ne sont pas artiniens)? Nous avons souhaité répondre un peu plus en termes de fondement à cette question. En fait, elle est essentiellement symétrique et l'effacement est bien total, dès lors qu'on s'autorise la souplesse de "à quelques cardinaux près".

Pour formaliser, nous noterons *indice d'artinianité (resp noethérianité)* de l'anneau A le plus petit ordinal κ tel qu'il n'existe pas d'application strictement croissante de $(\kappa, \in)$ dans $(Ideaux(A), \supset)$ (resp $(\kappa, \in)$ dans $(Ideaux(A), \subset)$). Le théorème suivant[3] montre que la structure annelée + la commutativité[4] écrase la distinction entre la "tendance à la bonne fondation" de $\leq$ et celle de $\geq$ pour des ordres "fondamentaux" (ie d'un type dont on pourrait éventuellement espérer qu'ils implémentent le temps dans des progrès futurs de la correspondance de Curry-Howard

Théorème 141 *(ZFC + CM[5]) Pour tout cardinal a il existe un cardinal b tel que pour tout anneau commutatif A si l'un de ses indices d'artinianité ou de neothérianité est $\leq a$ alors son autre indice est $\leq b$.*

[3]Nous en avons mis une preuve sur HAL (voir [Cha5], car elle est un peu longue pour figurer dans le présent texte
[4]La commutativité est nécessaire, nous avons signalé dans [Cha5] des exemples canoniques quand elle n'est pas supposée!!
[5]désigne classiquement l'axiome : il existe un Cardinal Mesurable

Chapitre 7

Tukey inoffensivité des degrés ludiques

7.1 Introduction

Dans ce chapitre, on étudie un problème unique, qui est presque un exemple, mais qui donne une idée plus précise des questions soulevées par le paradigme téléphonique: on se demande quelle puissance ludique est nécessaire pour “acheter” le passage d’une puissance Tukey a à une puissance Tukey b. On verra dans le chapitre 8 que l’augmentation de l’espérance de gain à des jeux de type casino via l’utilisation d’un téléphone ludique **n’est pas possible à moins que ce téléphone ne soit assez puissant**. Ce "assez puissant" inclut l’impossibilité d’être fabriquée par la théorie quantique. On se demande si la notion de "Tukey-puissance" diffère suffisamment ou non de la notion "capacité à augmenter son espérance de gain". Ce sont des notions différentes, bien qu’ayant trait toutes les deux à la catalyse de l’information. De manière surprenante, on va s’apercevoir que les degrés de Tukey sont suffisamment généraux pour que tout téléphone ludique (c’est à dire toute capacité de quelque nature que ce soit) qui n’est pas trivial parvienne à catalyser AU MOINS une information X vers une information Y, alors que X n’est pas au moins aussi bonne que Y. **Il en découle que la notion d’information ne peut pas être saisie complètement par la démarche probabiliste** et ce, de manière objective. Le résultat est suffisamment robuste pour valoir **même si on n’admet pas l’existence de l’infini mathématique**. Il concerne donc "la vie de tous les jours".

Soient $a := (E, F, R)$ et $b := (U, V, S)$ deux relations. On rappelle que $injvirt(a, b)$ désigne le représentant ludique du téléphone à deux combinés décrit par:

- Clavier du combiné1: E
- Clavier du combiné2: V
- Ecran du combiné1: U
- Ecran du combiné2: F
- Garantie: ensemble des $((e, u), (v, f))$ tels que $[(e, f) \in R$ ou $(u, v) \notin S]$.

Cette définition est fondée sur le lemme suivant:

Lemme 142 *$injvirt(a, b)$ est trivial si et seulement si $a \leq_{tuk} b$*

Preuve : Cela résulte immédiatement des définitions.

Il est donc intéressant d'étudier une notion intuitivement proche de celle-ci, mais dont la description est différente syntaxiquement: On conserve les notations précédentes.

Alice et Bob sont séparés et ne peuvent que s'envoyer un seul "message" en utilisant un téléphone ludique T à deux combinés, Alice disposant du combiné1. On note $((E_1 \times F_1) \times (E_2 \times F_2), G)$ la garantie de T.

On impose à Alice un certain $x \in E$. Elle dispose d'un téléphone de Tukey b-garanti pour envoyer un message à Bob. Mais n'oublions pas que notre paradigme nous autorise à ignorer les contraintes de temps. Alice peut donc, aussi, taper sur le clavier du combiné1 de son téléphone et attendre de voir l'écran pour envoyer un b-message à Bob. De même, Bob peut attendre d'avoir reçu son b-message pour taper sur son clavier de combiné2. A la vue de son écran, il devra proposer un $z \in F$. Finalement, l'équipe Bob-Alice gagne ce protocole quand $(u, v) \in S$.

L'existence d'une stratégie infaillible se formalise comme suit:
Il existe $f \in ((E \times F_1) \to U)$, $g \in (E \to E_1)$, $h \in V \to E_2$ et $k \in ((V \times F_2) \to F)$ tels que
pour tous $x \in U,\ y \in V,\ (r_1, r_2) \in F_1 \times F_2$,
si $((g(x), r_1), (h(y), r_2)) \in G$ et $(f(x, r_1), y) \in S$ alors $(x, k(y, r_2)) \in R$

Autrement dit, en se servant d'un b-téléphone de Tukey et du téléphone T, l'équipe Alice-Bob a été capable de simuler l'envoi d'une a information. Quand une telle stratégie infaillible existe, on dira que le triplet (T, a, b) est en situation de catalyse.

L'objectif de la section suivante est de caractériser la classe des T qui sont tels que (T, a, b) est en catalyse

7.1.1 Caractérisation des ludiques qui catalysent des Tukey

On a envie de conjecturer que (T, a, b) est en situation de catalyse si et seulement si $T \geq injvirt(a, b)$.

Lemme 143 *Le triplet $(injvirt(a, b), a, b)$ est en situation de catalyse*

Preuve : Décrivons la stratégie de l'équipe Alice-Bob en gardant les notations de la section précédente:

- $f : (x, r_1) \mapsto r_1$
- $g : x \to x$
- $h : y \to y$
- $k : (y, r_2) \to r_2$

Ainsi, voyant x Alice le tape sur la clavier du combiné1. Voyant la réponse r_1 qui ici est un élément de U, elle utilise son b-téléphone pour l'émettre. Bob, qui reçoit $y \in V$ tel que $(r_1, y) \in S$, sur son Tukey-téléphone b-garanti, tape alors y sur son clavier de combiné2 de T et reçoit $r_2 \in F$. Il annoncé r_2. La garantie de T est que si $(r_1, y) \in S$ (et ici c'est bien le cas) alors $(x, r_2) \in R$. Il s'ensuit que l'équipe gagne.

On s'interroge maintenant sur une éventuelle réciproque: on note $((E_1 \times F_1) \times (E_2 \times F_2), G)$ la garantie d'un téléphone T tel que (T, a, b) est en situation de catalyse. En gardant les noms utilisés dans le paragraphe précédent, on suppose que qu'il existe une stratégie (f, g, h, k) pour l'équipe Alice-Bob, ie, telle que pour tous $x \in U; y \in V; (r_1, r_2) \in F_1 \times F_2$:

si $((g(x), r_1), (h(y), r_2)) \in G$ et $(f(x, r_1), y) \in S$ alors $(x, k(y, r_2)) \in R$

Ceci **est exactement** la définition de $T \geq_{lud} injvirt(a, b)$ dès lors qu'on a en tête qu'il y a équivalence propositionnelle entre les deux énoncés suivants:

- *Si A alors si B alors C*
- *Si A et B alors C*

On a donc:

Théorème 144 *Pour tout représentant de degré ludique d'uplicité2, tous représentants a, b de degrés de Tukey: (T, a, b) est en catalyse si et seulement si $T \geq_{ludique} injvirt(a, b)$*

7.2 Degrés ludiques Tukey-inoffensifs

La section présente est consacrée à une définition et une question:

Définition 145 *Soit T représentant de degré ludique d'uplicité2. On dira qu'il est Tukey-inoffensif quand pour tous représentants de degrés de Tukey a, b : si $T \geq injvirt(a, b)$ alors $a \geq_{tuk} b$*

Question 146

- *Quelle puissance maximale peut-on atteindre avec un Tukey-inoffensif?*
- **Existe-t-il des Tukey-inoffensifs qui ne sont pas FMQ[1]?**
- **Existe-t-il des FMQ qui ne sont pas Tukey inoffensifs?**

La section suivante tente d'aller un peu plus loin dans la compréhension de ce que ne peuvent pas faire les Tukey-inoffensifs.

7.2.1 Un exemple

Le degré du téléphone suivant est très faible, malgré son caractère impressionnant:

Définition 147 *Soit E, F deux ensembles. Soient $E_1 := E_2 := E$ et $F_1 := F_2 := F$ et $G := \{((x_1, y_1), (x_2, y_2)) \in (E_1 \times F_1) \times (E_2 \times F_2) \mid x_1 = x_2 \iff y_1 = y_2\}$. On appelle ce représentant le coloriage de E par F et on le note $color(E, F)$*

[1] La définition de FMQ est donnée dans le chapitre suivant

Le théorème suivant informe sur sa faiblesse (même si E est un très gros ensemble et $F = 2$)

Théorème 148 *Si $card(F) \geq 2$ alors $color(E, F)$ est casino-inoffensif*[2].

Preuve : il suffit de le prouver quand $F = 2$. On définit $p(x, i, y, j)$, pour $(x, y) \in E^2$, $(i, j) \in \{0, 1\}$ par:

$$if\ x = y\ then\ if\ i \neq j\ then\ 0\ else\ \tfrac{1}{2}\ else\ if\ i = j\ then\ 0\ else\ \tfrac{1}{2}$$

.

La relation $p \neq 0$ est $color(E, F)$ et elle est casino-inoffensive.

Cette écriture abstraite "officielle" ne dit pas de manière imagée à quel point ce téléphone (par exemple, prenons le cas $color(100, 2)$) est "faible" **pour ses utilisateurs**. Lorsqu'Alice et Bob s'en servent, le démon caché dans le téléphone regarde s'ils ont tapé la même touche et tire au sort un couple (i, i) si oui, et un couple $(i, 1 - i)$ sinon de manière uniforme et équiprobable. Tant qu'Alice et Bob n'ont accès qu'à ces réponses aléatoires, ils ne peuvent rien en faire.

Cependant, on a le lemme:

Lemme 149 *$color(E, F)$ est trivial si et seulement si $card(E) \leq card(F)$*

Preuve : C'est évident, puisque c'est une recopie des définitions.

Virtuellement, $color(100, 2)$ colorie une clique à 100 sommets avec deux couleurs. Soit E un ensemble. Intéressons-nous à $T := color(E, 2)$. Pour ce faire, on va s'intéresser à deux degrés de Tukey bien particuliers.

Définition 150 *Soit n un entier naturel. On note $cv(n, X) :=$ l'ensemble des parties de X dont le cardinal est au plus n. On note $couv(n, X)$ le représentant $couv(n, X) := (X, cv(n, X), \in)$*

7.2.2 Tukey-offensivité de T

Dans cette sous-section, $T := color(E, 2)$. On cherche à répondre à la question: *T est-il Tukey-offensif?*

Lemme 151 *$color(E, 2) \geq_{lud} injvirt(couv(2, E), couv(3, E \times 2))$*

Preuve : On l'écrit, comme souvent, de manière imagée pour que le lecteur ait plus de facilité à l'apprécier. On note:

- $a := couv(2, E)$
- $b := couv(3, E \times 3)$

[2] La définition de casino-inoffensif est donnée dans le chapitre suivant

Alice dispose du combiné1 de T et d'un b-téléphone de Tukey. Bob du combiné2 (il est éloigné d'Alice).

On impose à Alice $x \in E$. Le but d'Alice est, en se servant de b et de T, d'envoyer à Bob un a-message, c'est à dire un ensemble contenant au plus deux éléments et dont x est un élément. Voici la stratégie qu'elle va suivre: elle tape x sur le clavier du combiné1 de T. Elle reçoit $i \in 2$. Elle émet le couple (x, i) sur son b-téléphone. Bob reçoit alors un ensemble S ayant au plus 3 éléments et dont (x, i) fait partie. Notons $(y, i); (z, i); (t, j)$ ces trois couples reçus, ie $S = \{(y, i); (z, i); (t, j)\}$.

La répétition du petit i vient du fait que la deuxième projection appartient à 2 et on ne perd donc pas en généralité, car il y a au moins deux des deuxièmes projections égales parmi les 3 reçues. On peut supposer $y \neq z$ sinon Bob peut annoncer $m := \{y; z; t\}$ et gagner puisqu'alors $x \in m$ et $m \in cv(2, E)$. Bob range ainsi comme nous ces trois couples. Il décide alors de taper y sur son combiné2-clavier. Sur son écran s'affiche $k \in 2$. Il fait alors le pari suivant:

- if $k = i$ then annoncer $\{y; t\}$
- if $k \neq i$ then annoncer $\{z; t\}$

Dans tous les cas l'équipe Alice-Bob vient de simuler l'envoi d'un a-message à l'aide de T et d'un b-téléphone

Pour chaque E, il suffit de prouver que $couv(3, E \times 2)$ n'est pas supérieur ou égal à $couv(2, E)$ pour en déduire que $color(E, 2)$ est Tukey-offensif. Evidemment, si $card(E) \leq 2$ alors le degré de Tukey de $couv(2, E)$ est le bottom des Tukey et le degré ludique de $color(E, 2)$ est le bottom des ludiques d'uplicité2.

Lemme 152 *Soient E, F des ensembles. Si $couv(2, E) \leq couv(3, F)$ alors $card(E) \leq 2$.*

Preuve :

Soit un dessin de réduction

$$x \in E \to f(x) \in F \mid H \in cv(3, F) \to g(H) \in cv(2, E)$$

de $couv(E, 2)$ à $couv(3, F)$. On peut supposer que $card(F) \geq 4$ et que f est surjective sans perte de généralité, ce qui entraine que $card(E) \geq 4$. Soit $S := \{x_1, x_2, x_3\}$ un ensemble de cardinal 3, inclus dans E tel que la restriction de f à S est injective. Tous les éléments de S sont des éléments de $g(S)$. Or cela est contradictoire avec le fait que $card(g(S)) \leq 2$.

Finalement:

Théorème 153 *Soit E un ensemble. Si $color(E, 2)$ est Tukey-inoffensif alors $card(E) \leq 2$ et donc $color(E, 2)$ est trivial*

Il reste une question abstraite que nous n'avons pas élucidée: *existe-t-il des ludiques non triviaux qui sont Tukey-inoffensifs?*

7.3 Tout degré ludique Tukey-inoffensif est trivial!

Nous allons le prouver dans les paragraphes suivants. Avant précisons quelques angles de vue.

7.3.1 Diverses approches philosophiques de la question

Du fait que les mathématiques utilisent sans complexe l'infini, il faut avouer que la question et sa réponse peut avoir plusieurs interprétations. Les degrés canoniques du genre “anticantor”, bien que non triviaux, sont tellement faibles (dès lors qu'ils sont sur des supports infinis) qu'ils deviennent sans difficulté triviaux dans une extension générique. Un sceptique un peu trop finitiste dans ses opinions aurait donc quelques réserves face à un même degré qui passe de non trivial à trivial selon l'univers qui le regarde. Nous allons donc prouver deux théorèmes:

- l'un dira que tout degré ludique non trivial de support fini est Tukey inoffensif dans un sens fort, à savoir qu'il collapse deux degrés de Tukey qui ne sont vus collapsables par aucun sur univers.
- L'autre dira que tout degré ludique non trivial est Tukey offensif.

En fait, le premier théorème dira que si a est un degré ludique non trivial de support fini alors il existe des degrés de Tukey **de supports finis tous les deux**, tels que $non(b \geq_{tuk} c)$ et pourtant tels que un a-téléphone permet de catalyser (b, c), ie permet de se servir d'un b téléphone (en plus du a téléphone) pour envoyer un c-message. Comme tout est de support fini ici, le forcing ne changera pas la donne et le résultat est absolu [3]

Soit E, F deux ensembles finis. On rappelle la garantie "anticantor(E,F)" et le rôle particulier qu'elle joue:

Définition 154 *Le téléphone anticantor(E, F) est défini par:*

- *Il a deux combinés*
- *Les touches du clavier du combiné1 sont les éléments de $E \to F$*
- *Les lampes de l'écran du combiné1 sont les éléments de E*
- *Les touches du clavier du combiné2 sont les éléments de E*
- *Les lampes de l'écran du combiné2 sont les éléments de F*
- *La garantie est l'ensemble des $((f, s), (x, r)) \in ((E \to F) \times E) \times (E \times F)$ tels que $s \neq x$ ou $f(s) \neq r$*

On rappelle la propriété spectaculaire de ces téléphones:

[3] Soit n un ensemble fini et $G \subseteq \prod_{i \in n}(E_i \times F_i)$ une garantie ludique d'uplicité n. On note $a := (I, (i \mapsto (E_i, F_i), G))$. On dit que le représentant de degré ludique a est forçable quand il existe une extension générique V_2 de l'univers V et des applications $i \in n \mapsto f_i \in (E_i \to F_i)$ tels que pour tout $x \in \prod_i E_i : [i \mapsto (x_i, f_i(x_i))] \in G$. Cette façon de décrire de manière externe la forçabilité est selon des résultats classiques équivalente à la manière interne suivante:

Il y a équivalence pour a entre être forçable et le fait que Alice n'ait pas de stratégie gagnante au jeu suivant: *à chaque étape, Alice choisit $i \in n$ et $x \in E_i$ et Bob répond par $y \in F_i$. Si le couple (i, x) a déjà été joué à une étape précédente, Bob a le devoir de redonner la même réponse. Les deux joueurs construisent ainsi des fonctions partielles f_i^p de support fini telles que pour deux étapes quelconques p, q si $p > q$ alors pour chaque $i \in n$: f_i^p prolonge f_i^q. Alice gagne si à une étape p, il existe $i \mapsto x_i \in dom(f_i^p)$ tel que $[i \mapsto (x_i, f_i^p(x_i))] \notin G$*

Théorème 155 *Pour tout représentant r de degré ludique non trivial de support fini à deux combinés, il existe E fini tel que $anticantor(E,E) \leq_{lud} r$. En outre, quelques soient les ensembles E,F (finis ou non), $anticantor(E,F)$ n'est pas trivial. (On a aussi que pour tout représentant r de degré ludique non trivial à deux combinés, il existe un ensemble E tel que $anticantor(E,E) \leq_{lud} r$).*

On a déjà prouvé ce théorème dans un chapitre précédent. Il exprime la co-initialité de la classe des anticantor dans les degrés ludiques

7.4 Supports finis

7.4.1 Enoncés du lemme et du théorème

Le lemme suivant établit, de manière absolue (ie insensibilité au forcing), que la Tukey offensivité est inévitable.

Lemme 156 *Soit E,F finis. Alors il existe deux représentants de degrés de Tukey de supports finis a,b tels que $anticantor(E,F)$ est ludiquement supérieur ou égal à l'injection virtuelle de a dans b et a,b sont pourtant tels que b n'est pas Tukey-supérieur ou égal à a*

La conséquence de ce lemme, est, quand on le marie à la co-initialité des anticantor, que:

Théorème 157 *Soit R un représentant de degré ludique d'uplicité 2 de support fni. Alors il existe deux représentants de degrés de Tukey de supports finis a,b tels que R est ludiquement supérieur ou égal à l'injection virtuelle de a dans b et a,b sont pourtant tels que b n'est pas Tukey-supérieur ou égal à a*

7.4.2 Preuve du lemme (version finitiste)

Preuve : Les degrés de Tukey que nous allons considérer sont les suivants: soit E,F deux ensembles finis. On abrège $A := E \times F$ et $T :=$ l'ensemble des parties de A dont le cardinal est au plus celui de E. Soit $R :=$ l'ensemble des couples $(X,u) \in T \times A$ tel que $u \notin X$. On note $a := (T,A,R)$, qui est un représentant de degré de Tukey. Il est évident que I_E n'est pas $\geq_{tuk} a$. On va prouver que $e := anticantor(E,F)$ est ludiquement supérieur ou égal à l'injection virtuelle de a dans I_E.

Pour le confort du lecteur, on décrit l'argument en termes Alice-Bob. Alice dispose d'un e téléphone ludique et d'un I_E téléphone de Tukey. Elle souhaite s'en servir intelligemment pour envoyer un a message de Tukey à Bob. L'adversité impose un $X \in T$ à Alice. Alice est face à une alternative: ou bien X est un graphe de fonction de E dans F, définie sur E (cas1). Ou bien non (cas2). La finitude entraine que dans le cas2, il existe $x \in E$ tel que pour tout $y \in F : (x,y) \notin X$. Dans ce cas, Alice transmet à Bob, en utilisant I_E un tel x. Bob le tape alors sur son clavier de combiné2 du e-téléphone et reçoit r. Il sait alors que $(x,r) \notin X$. Dans le cas1, $X \in (E \to F)$. Alice tape X sur son clavier de combiné1 du e-téléphone et reçoit $s \in E$. Elle transmet à Bob, via son I_E-téléphone ce s à Bob. Bob tape alors $x := s$ sur son clavier de combiné2 du e-téléphone et reçoit r. Il sait qu'alors $(x,r) \notin X$

7.5 Supports quelconques

7.5.1 Enoncés du lemme et du théorème

La démonstration précédente, qui utilise une propriété bien singulière de la finitude, ne donne aucune idée évidente de généralisation à la situation infinie. De plus, un anticantor de support infini étant, dans le cas général, forçable, on peut être certain qu'aucun argument absolu ne peut marcher. On a pourtant, comme dans le cas fini, les lemmes et théorème suivants:

Lemme 158 *Soit E, F quelconques. Alors il existe deux représentants de degrés de Tukey a, b tels que $anticantor(E, F)$ est ludiquement supérieur ou égal à l'injection virtuelle de a dans b et a, b sont pourtant tels que b n'est pas Tukey-supérieur ou égal à a*

La conséquence de ce lemme, est, quand on le marie à la co-initialité des anticantor, que:

Théorème 159 *Soit R un représentant de degré ludique d'uplicité 2. Alors il existe deux représentants de degrés de Tukey a, b tels que R est ludiquement supérieur ou égal à l'injection virtuelle de a dans b et a, b sont pourtant tels que b n'est pas Tukey-supérieur ou égal à a*

7.5.2 Preuve du lemme (version infinitiste)

Preuve : La construction est très différente de celle de la situation finie. On est face à deux ensembles E, F et on veut montrer que le téléphone à deux combinés qui garantit $\{((x,r),(f,s)) \in (E \times F) \times ((E \to F) \times E) \mid f(x) \neq r \text{ ou } s \neq x\}$ permet de catalyser deux degrés de Tukey a, b. On va considérer E comme un ensemble d'indices, et sans perte de généralité, E, F sont des cardinaux. Soient pour chaque $i \in E$ un cardinal régulier $k_i > E$ et $k_i > F$. La construction ressemble un peu à celle qui permet d'attester que les degrés de Tukey ont la propriété de la borne supérieure. On note P le produit des $k_i, i \in E$. Notons R la relation (Tukey) suivante: Alice envoie un couple $((x,i),r)$ où $i \in E$ et $x \in k_i$ et $r \in F$. Bob reçoit $(y,t) \in P \times F^E$ tel que $y_i > x$ ou $t_i = r$. Notons S la relation (Tukey) suivante: Alice envoie $(x,i) \in k_i \times E$; Bob reçoit $(y,s) \in P \times E$ tel que $y_i > x$ ou $s \neq i$.

La stratégie suivante permet à Alice, en se servant à la fois d'un téléphone ludique T d'uplicité2 $anticantor(E, F)$ et d'un Tukey-téléphone R de simuler un Tukey-téléphone S:

Il est imposé à Alice un couple (x,i) avec $i \in E$. Sur le combiné1 de T, Alice tape i. Elle reçoit $r \in F$. Elle se sert ensuite de son R-Tukey-téléphone pour envoyer $((x,i),r)$. Bob reçoit un couple (y,t) où $t \in E \to F$ et $y \in P$ qui sont tels que $y_i > x$ ou $t_i = r$. Bob utilise alors le combiné2 de son téléphone T en y tapant t. Il reçoit $s \in E$. Il proclame (y,s). Supposons qu'on n'a pas $((x,i),(y,s)) \in S$: alors on n'a pas $y > x_i$ et on n'a pas non plus $s \neq i$. Cela contredit la garantie de T car $t_i = r$ et $i = s$. Il reste à justifier qu'on n'a pas $S \leq_{Tukey} R$. Dessinons ce que doit être une réduction:

$$(x,i) \to ((x'(x,i), i'(x,i)), r(x,i)) \mid (y,t) \to (y'(y,t), s'(y,t))$$

avec l'implication $y(i'(x,i)) > x'(x,i)$ ou $t(i'(x,i)) = r(x,i)$ entraine $y'(y,t)(i) > x$ ou $s'(y,t) \neq i$

En termes de notation, c'est lourd à lire. Mais l'incomparabilité entre les k_i va produire de grosses contraintes: en effet, pour chaque $i \in E$, il existe une partie non bornée B_i de k_i, un élément $y_i \in k_i$ et un élément $t_i \in F$, de sorte que: pour tout i dans E et x dans $B_i : r(x,i) = t_i$; de plus, si $j := i'(x,i) \neq i$ alors $y_j > x'(x,i)$. Posons $y_2 := y'(y,t)$. Regardons le couple $(y_2, j := s'(y,t))$. Soit $x \in B_j$ tel que $x > y_2(j)$. Comme on n'a pas $s'(y,t) \neq j$, il s'ensuit qu'on n'a pas

$((x'(x,j),i'(x,j)),r(x,j))R(y,t)$. Donc $t(i'(x,j)) \neq r(x,j)$; donc $i'(x,j) \neq j$ ce qui entraine $y(i'(x,j)) > x'(x,j)$ qui entraine $y_2(j) > x$ donc une contradiction

Chapitre 8

Caractérisations de classes importantes

8.1 Introduction

Dans ce chapitre, nous étudions certains types de téléphones à deux combinés. Dans la suite, *garantie* signifie une partie $R \subseteq (E_1 \times F_1) \times (E_2 \times F_2)$. *Dans ce chapitre, sauf dans les cas où ça génèrerait de l'ambiguité, on identifiera:* $(A \times B) \times C$ *à* $A \times B \times C$ *et* $((x, y), z)$ *à* (x, y, z)

8.2 Définition des degrés FMQ

Définition 160 *Soit* E *un espace hermitien de dimension* p *et* f *une forme* n*-linéaire non nulle sur* E*. On note* $TelFMQ(E, f, n) :=$ *l'ensemble des* $((b_1, i_1), (b_2, i_2), .., (b_n, i_n))$ *tels que tous les* b_i *sont des bases orthogonales de* E *et tous les* i_k *sont des éléments de* p *et* $f(b_1(i_1), ..b_n(i_n)) \neq 0$.

Un degré d'arité n *est dit FMQ s'il est ludiquement réductible à au moins un téléphone de la forme* $TelFMQ(E, f, n)$

Cette "froide" définition fonde son intérêt sur le théorème de Kochen-Specker [1](corollaire du théorème de Gleason). L'expérience d'Aspect avait donné dans les années 1982 une première confirmation expérimentale d'une affirmation reproductible plus faible que le plein théorème de KS.

Les premières vraies confirmations, dénuées de toute sur-couche probabiliste sont apparues dans les années 1990, GHZ[2] étant probablement une sorte "d'apothéose" dans la simplicité du téléphone confirmé. De nombreuses autres expériences (avec des téléphones à DEUX combinés) ont confirmé les prédictions quantiques.

---

[1] Ce théorème démontre que toute théorie à variables cachées rendant compte des résultats des expériences de physique quantique est contextualiste, c'est-à-dire que les valeurs mesurées des paramètres physiques dépendent nécessairement du contexte expérimental, et non des entités physiques seules. Ce théorème porte un autre coup à la vision réaliste d'Einstein, qui supposait que chaque entité physique a une existence objective, indépendante de son environnement et de l'observation. Voir [Del]

[2] l'expérience de Greenberger Horne et Zeilinger offre un exemple de téléphones quantiques à trois combinés, dont le viol de la localité est peut-être didactiquement le plus simple et le plus spectaculaire, et il est un exemple où aucune considération probabiliste n'intervient

8.2.1 Informatisation

Dans cette sous-section, on dira qu'une relation ludique est entièrement finie quand "tout est fini" dans sa définition: le nombre de combinés, les écrans, les claviers. Les garanties ludiques entièrement finies se prêtent à une question intéressantes technologiquement qui est celle de les reconnaitre "automatiquement" grâce à l'outil informatique.

Il semble hélas que ce soit une question difficile. La définition ci-dessus montre que

Théorème 161 *L'ensemble des garanties ludiques FMQ entièrement finies est* **récursivement énumérable**

On a envie de conjecturer que c'est en fait un ensemble **récursif**. Hélas, il semble que cet énoncé soit relié à un autre qui est un problème ouvert:

Théorème 162 *Supposons la conjecture généralisée de Connes-Kirchberg*[3] *. Alors l'ensemble des garanties FMQ entièrement finies est* **CO-récursivement énumérable** *et donc* **récursif**

La démonstration qui suit est due à Anatole Khélif.

Preuve : Pour simplifier, on se restreindra au cas d'uplicité 2, le cas général se montrant de la même manière. Soit R une garantie correspondant à un degré ludique FMQ ($R \subseteq (E_1 \times F_1) \times (E_2 \times F_2)$).D'après la définition de FMQ, par identification de $V \bigotimes V$ avec $(L)(V,V)$,il existe un espace vectoriel hermitien de dimension finie V et un élément unitaire v de $V \bigotimes V$ et des projecteurs orthogonaux $p(x_1, y_1)$ avec $(x_1, y_1) \in (E_1 \times F_1)$ et $q(x_2, y_2)$ avec $((x_2, y_2) \in (E_2 \times F_2)$ tels que les $p(x_1, y_1)$ commutent avec les $q(x_2, y_2)$ (ils agissent chacun sur un des termes du produit tensoriel).Avec de plus les propriétés suivantes: pourx_1 fixé la somme des $p(x_1, y_1)$ est id, pourx_2 fixé la somme des $q(x_2, y_2)$ est id.La garantie de R s'exprime par le fait que si $(x_1, y_1, x_2, y_2)) \notin R$ alors $p(x_1, y_1)q(x_2, y_2)(v) = 0$. Appelons $T_R)$ la moyenne des $Id - p(x_1, y_1)q(x_2, y_2)$ pour$(x_1, y_1, x_2, y_2)) \notin R$, nous obtenons $T_R)(v) = v$. Comme $T_R)$ est de plus une moyenne de projecteurs orthogonaux, il s'ensuit que sa norme opératorielle est exactement égale à 1.Pour prouver que l'ensemble des l'ensemble des garanties FMQ entièrement finies est **CO-récursivement énumérable**,l'idée est de monter q'une relation non FMQ sera associée à un opérateur de type $T_R)$ de norme strictement petite que 1 et que cette inégalité normique stricte est algorithmiquement vérifiable.Pour faire intervenir une $C*$-algèbre de type $C(G)$, il faut d'abord écrire les projecteurs comme moyennes d'opérateurs unitaires. Nous procédons de la manière suivante: soit par exemple n le cardinal de F_1, il existe alors une bijection j de F_1 dans n. Pour x_1 élément fixé de E_1, choisissons une racine primitive n-ième ξ de l'unité et faisons la somme des $(\xi^j(y))p(x_1, y)$ pour y variant dans F_1. Nous obtenons alors un opérateur unitaire dont la puissance n-ième est l'identité et que l'on notera $U_1(x_1)$.Nous procédons de la même manière pour tout élément x_2 élément fixé de E_2 et nous notons $U_2(x_2)$ l'opérateur correspondant.Dans ce casnous obtenons que $(\frac{1}{n}\sum_{i=1}^{n} \xi^(-ki)U_1^i = p(x_1, y_1)$ pour $k = j(y_1)$. Nous faisons de même avec les $q(x_2, y_2)$ le cardinal m de F_2 jouant le rôle de n pour F_1.En fait nous préférons exprimer les $p(x_1, y_1)$ sous la forme $(\frac{1}{n^2}\sum_{i=1}^{n} \xi^(-ki)U_1(x_1)^i \sum_{i=1}^{n} \xi^(ki)U_1(x_1)^-i = p(x_1, y_1)$. La positivité et le caractère autoadjoint de l'expression ne dépend alors plus que du caractère unitaire de $U_1(x_1)$.Faisons maintenant la moyenne de $T_R)$ avec la moyenne des opérateurs unitaires suivants $Id)$, les $U_1(x_1)^n$, les $U_1(x_1)^-n$, les $U_2(x_2)^m$ et les $U_2(x_2)^-m$. Nous obtenons un opérateur que nous appelons $Op(R)$.En tant que moyenne d'opérateurs de norme au plus égale à 1, $Op(R)$ est de norme au plus égale à 1. Comme, par construction $Op(R)(v) = v$,$Op(R)$ est de norme exactement égale à 1.Soit maintenant G_1 le groupe libre dont les générateurs sont indexés par les éléments deE_1 et G_2 le groupe libre dont les générateurs sont indexés par les élélments deE_2.Considérons maintenat la $C*$-algèbre $C(G_1 \times G_2)$ munie de la norme maximale.Considérons maintenant l'équivalent de $Op(R)$ dans la $C*$-algèbre $C(G_1 \times G_2)$,les générateurs de G_1 jouant le rôle des $U_1(x_1)$ et ceux de G_2 jouant le rôle des $U_2(x_2)$.Appelons le aussi $Op(R)$.Par construction ce $Op(R)$ est de norme au plus égale à 1.Comme par construction aussi les$U_1(x_1)$ commutent avec les $U_2(x_2)$ et que ce sont ous des opérateurs unitaires, le $Op(R)$ initial est l'image du $Op(R)$ de la $C*$-algèbre par une représentation de dimension finie. comme cette image est de norme 1 nous

[3] Conjecture généralisée de Connes Kirchberg: Soit G un produit fini de groupes libres à nombre fini de générateurs, alors la norme d'un élément$u$ de la $C*$-algèbre $C(G)$ est le sup des normes des images de u par toutes les représentations de dimension finie de $C(G)$, ce sup étant atteint si u est une combinaison linéaire finie à coefficients complexes d' éléments de G.

pouvons en conclure que le$Op(R)$ de la $C*$-algèbre est de norme exactement égale à 1.Réciproquement,soit R une garantie($R \subseteq (E_1 \times F_1) \times (E_2 \times F_2)$), soit$G_1$ et G_2 définis comme précédemment. Montrons que si le $Op(R)$ de la $C*$-algèbre $C(G_1 \times G_2)$ est de norme exactement égale à 1, alors R est FMQ. D'après la conjecture généralisée de Connes Kirchberg, comme $Op(R)$ est une combinaison linéaire finie d'éléments de$(G_1 \times G_2)$, il existe un représentation de $C(G_1 \times G_2)$ de dimension finie telle que l'image de $Op(R)$ soit de norme exactement égale à 1. Comme il s'agit d'une moyenne d'opérateurs qui par construction sont de norme au plus égale à 1, il s'ensuit qu'il existe un espace vectoriel de dimension finie H et un vecteur unitaire h de H tel que l'image de chacun de ces opérateurs sur$h$ vaut h (cas d'égalité dans l'inégalité triangulaire pour un espace hermitien).Il est bien connu que toute repérsentation de dimension finie de $C(G_1 \times G_2)$ ($C*$-algèbre d'un produit de groupes) de dimension $finie$ se ramène au produit tensoriel d'une représentation de $C(G_1)$ et d'une représentation de $C(G_2)$.Certes les équivalents des $p(x_1, y_1)$ et des $q(x_2, y_2)$ ne sont plus de "vrais" projecteurs mais en remplaçant ces équivalents par la projection sur le sous-espace propre associé à 1 de ces équivalents.Il ne rest plus qu'à associé (x_1 une base orthogonale contenant les bases des sous espaces propres associés à 1 des $p(x_1, y_1)$, de faire de même avec les (x_2 et les $q(x_2, y_2)$ et d'identifier le vecteur h au f de la définition des garanties FMQ.Donc pour vérifier qu'une garantie R n'est pas FMQ, il suffit de vérifier que $Op(R)$ est de norme strictement plus petite que 1.Peut-on le faire automatiquement? C'est là que le théorème de Théorème de Russo-Dye intervient. La norme d'un opérateur est l'inf des somme demodule de coefficients quand on écrit cet opérateur comme combinaison linéaire d'opératures unitaires.Par calcul fonctionnel, on peut même supposer que ces opérateurs unitaires sont des exponentielles d'opérateurs antiautoadjoints.Compte tenu de la convergence normale de la série exponentielle, on peut verifier que la norme d'un opérateur est stictement plus petite que 1 à un ordre finie de développement des séries exponentielles.Il s'ensuit que l'ensemble des garanties FMQ entièrement finies est bien **CO-récursivement énumérable** et donc **récursif**.

La possibilité d'une reconnaissance automatique du caractère FMQ d'une garantie entièrement finie est actuellement un problème ouvert(en 2014).

8.3 Téléphones casino-inoffensifs à deux combinés

Lorsque vous vous rendez au casino, il n'y a rien, à priori qui vous garantit que le casino ne triche pas. La faiblesse des téléphones (à deux combinés) que nous étudions est telle, nous l'avons vu, qu'ils ne permettent pas de transmettre d'information d'un combiné à l'autre, sauf s'ils sont TSD.

Est-ce pour autant dire qu'un téléphone non TSD n'aurait pas quelque autre avantage de nature légèrement différente, qui attesterait sa non localité?

L'idée qui suit décrit un protocole qui permettrait d'exprimer, sans appel, qu'un téléphone a une puissance réelle, puissance pourtant suffisamment faible pour qu'il ne puisse pas transmettre de l'information.

Supposons qu'on dispose d'un téléphone à deux combinés C_1, C_2 disposant chacun d'un clavier et d'un écran. Nos joueurs Alice et Bob vont s'en servir pour proposer à un casino un compromis:

Afin de s'assurer que le casino "ne triche pas", il devra présenter son numéro gagnant à Alice. **Après quoi**, Alice (supposée séparée de Bob), utilisera son combiné C_1 pour "téléphoner" à Bob et faire tout ce qu'elle peut pour l'informer d'une "réalité" concernant ce numéro.

Bob et Alice se seront bien sûr accordés avant sur la stratégie d'utilisation, mais une fois qu'ils seront séparés, ils ne pourront plus se revoir avant la fin du jeu.

Si le téléphone est puissant, bien entendu Alice pourrait transmettre à Bob le numéro gagnant. Ou même un numéro qui ne gagne pas. Il s'agit d'une information, mesurée par le degré de Tukey $\{(x, y) \in E^2 \mid x \neq y\}$ dont on sent intuitivement que si E est fini alors même cette petite information devrait permettre à Bob, en un sens à préciser, d'augmenter son espérance de gain. En effet, **pouvoir éliminer un numéro parce qu'on sait qu'il n'est pas gagnant est déjà un avantage substantiel**.

Mais qu'en est-il de ce que permet, en termes d'espérance, un téléphone **nonTSD**?

C'est à cette question que nous allons répondre dans les sections qui vont suivre. Nous allons caractériser les téléphones trop faibles pour permettre l'existence d'une stratégie pour le couple (Alice,Bob) d'augmenter son espérance de gain. De manière peut-être surprenante, on verra qu'il y a beaucoup de téléphones non locaux qui ne permettent aucune augmentation d'espérance. D'ores et déjà, le lecteur peut imaginer les définitions qui vont émerger de cette intention d'étude technique du problème. La famille de jeux précédents sera appelée: *jeux de casinos surveillés par T*

La section suivante donne une définition plus technique et moins d'inspiration philosophique du mot *casino-inoffensif* déjà évoqué ci-dessus. *Pour des raisons techniques, le sens unique ne semble pas pouvoir se mathématiser facilement, c'est pourquoi nous étudierons un protocole symétrique où Bob,* **mais aussi Alice** *font des paris sur les numéros et sont tous deux ainsi, joueurs à part entière.* La question de la problématique du sens unique reste donc à ce stade ouverte .

8.4 Définitions plus techniques

Définition 163 *Soit R une garantie. On dira que R est préfortement non TSD quand:*

- *pour tous éléments x_1, y_1, x_2 respectivement de E_1, F_1, E_2 , il existe un élément $y_2 \in F_2$ tel que $((x_1, y_1), (x_2, y_2)) \in R$ et*
- *pour tous éléments x_2, y_2, x_1 respectivement de E_2, F_2, E_1 , il existe un élément $y_1 \in F_1$ tel que $((x_1, y_1), (x_2, y_2)) \in R$*

Cette propriété n'a pas de raison de passer à l'équivalence ludique. Donc plus généralement, on dira:

Définition 164 *R est fortement non TSD quand il existe S telle que $R \leq_{lud} S$ et S préfortement non TSD*

Attention, contrairement à un certain usage, ici préfortement implique fortement. La définition qui suit est une expression technique de la casino-inoffensivité:

Définition 165 *On suppose, ici F_1 et F_2* **finis**. *La garantie R est dite casino-inoffensive quand il existe une application p à valeurs dans $[0,1]$ avec les propriétés suivantes :*

1. *Pour tout couple $(x_1, x_2) \in E_1 \times E_2$, la somme des $p(x_1, x_2, y_1, y_2)$ quand y varie dans $F_1 \times F_2$ est égale à 1.*
2. *Pour un triplet (x_1, y_1, x_2), la somme des $p(x_1, x_2, y_1, y_2)$, y_2 variant dans F_2 ne dépend que du couple (x_1, y_1) , la propriété restant vérifiée si on permute les indices 1 et 2.*
3. *Pour tout quadruplet q si $p(q) \neq 0$ alors $q \in R$*

Remarque : La première définition inventorie les quadruplets qui sont tels que s'ils surviennent, ils informent un des utilisateurs des combinés d'au moins une touche que l'autre utilisateur **n'a pas** tapé sur son clavier. S'il existe de tels quadruplets alors la garantie n'est pas fortement non TSD. Partant d'une garantie, on peut retirer successivement les quadruplets évoqués ci-dessus, et itérer ces retraits. Ce qui reste à la fin fournit une garantie préfortement nonTSD ou infinie.

La deuxième définition, comme vue précédemment, met sous une forme "probabiliste" l'idée qu'on ne peut pas se servir d'un téléphone R-garantie pour augmenter son espérance de gain dans un casino où une inspection indépendante se servirait de R pour empêcher le casino de tricher. Les théorèmes suivants explicitent la nuance pour passer des casinos-inoffensifs aux fortement nonTSD:

8.5 Deux théorèmes caractérisant, en termes de multipermutable, les deux classes précédentes

On garde les conventions de la section précédente.

Théorème 166 *Les propriétés suivantes sont équivalentes:*

- R *est* **fortement non TSD**
- *Il existe un ensemble d'indices non vide* I *et des applications* f_1 *(respectivement* f_2*) de* E_1^I *dans* F_1^I *(respectivement de* E_2^I *dans* F_2^I*) tel que pour tout élément* x *de* E_1^I *et tout élément* x *de* E_2^I*, il existe des permutations* g_1 *et* g_2 *de* I *dans lui-même tel que pour tout* $i \in I$*:*

$$((x(g_1(i)), f1(x_1)(g_1(i))), (x(g_2(i)), f2(x_2)(g_2(i)))) \in R$$

Le théorème suivant est pratiquement un copié-collé du précédent, à ceci près qu'on a besoin de rajouter le mot *fini* et surtout on demande aux utilisateurs des claviers de tous taper la même touche. La casino-inoffensivité se caractérise donc par la multi-permut-alltable sur un nombre **fini** de tables.

Théorème 167 *Les propriétés suivantes sont équivalentes:*

- R *est* **casino-inoffensif**
- *Il existe un ensemble* **fini** *d'indices non vide* I *et des applications* f_1 *(respectivement* f_2*) de* E_1 *dans* F_1^I *(respectivement de* E_2 *dans* F_2^I*) tel que pour tout élément* x_1 *de* E_1 *et tout élément* x_2 *de* E_2*, il existe des permutations* g_1 *et* g_2 *de* I *dans lui-même tel que pour tout* $i \in I$*:*

$$((x_1, f_1(x_1)(g_1(i))), (x_2, f_2(x_2)(g_2(i)))) \in R$$

Les preuves de ces théorèmes vont s'appuyer sur deux lemmes:

8.5.1 Enoncé des lemmes

Lemme 168 *Soient* F_1 *et* F_2 *deux ensembles non vides. Soit* H *un ensemble infini de cardinal strictement plus grand que ceux de* F_1, F_2*. Soient* u_1 *(respectivement* u_2*) une surjection de* H *dans* F_1 *(respectivement* F_2*) telle que pour tout élément de* F_1 *(respectivement* F_2*) l'ensemble de ses antécédents par* u_1 *(respectivement* u_2*) soit un sous-ensemble de* H *de même cardinal que celui de* H*. Soit* $R \subseteq F_1 \times F_2$ *telle que:*

1. *pour tout élément* y_1 *de* F_1*, il existe* y_2 *élément de* F_2 *tel que* $(y_1, y_2) \in R$*.*
2. *pour tout élément* y_2 *de* F_2*, il existe* y_1 *élément de* F_1 *tel que* $(y_1, y_2) \in R$*.*

Alors *il existe une bijection* s *de* H *dans lui-même telle que pour tout* $(y_1, y_2) \in F_1 \times F_2$*:*
$(y_1, y_2) \in R$ *si et seulement si il existe* $h \in H$ *tel que* $[y_1 = u_1(h)$ *et* $y_2 = u_2(s(h))]$

Le deuxième lemme a un énoncé assez long:

Lemme 169 *Soient* F_1, F_2 *deux ensembles non vides finis. Soit* p *une une application de* $F_1 \times F_2$ *dans* $[0, 1]$ *telle que*

1. *la somme des* $p(y_1, y_2)$ *pour* (y_1, y_2) *variant dans* $F_1 \times F_2$ *est 1.*

2. *p ne prend que des valeurs rationnelles*

Soit H un ensemble fini dont le cardinal est multiple de tous les dénominateurs de fractions irréductibles représentant des valeurs prises par p. Soient u_1 (respectivement u_2) une application de H dans F_1 (respectivement F_2) avec les propriétés suivantes:

1. *pour tout élément y_1 de F_1 le nombre d'antécédents de y_1 par u_1 est le produit de la somme des $p(y_1, w)$ pour w variant dans F_2 par le cardinal de H.*

2. *pour tout élément y_2 de F_2 le nombre d'antécédents de y_2 par u_2 est le produit de la somme des $p(w, y_2)$ pour w variant dans F_1 par le cardinal de H*

Alors *il existe une bijection s de H dans lui-même telle que pour tout élément (y_1, y_2) de $F_1 \times F_2$, $p(y_1, y_2)$ est le rapport*

$$\frac{card(\{h|H : y_1 = u_1(h) \ et \ y_2 = u_2(s(h))\})}{card(H)}$$

La section suivante est consacrée à prouver les lemmes, celle qui la suit à prouver les théorèmes en admettant les lemmes.

8.6 Preuves des lemmes 168 et 169

8.6.1 Preuve du lemme 168

Soient F_1 et F_2 deux ensembles non vides. Soit R une relation binaire $R \in F_1 \times F_2$ vérifiant:

1) pour tout élément y_1 de F_1, il existe y_2 élément de F_2 tel que $(y_1, y_2) \in R$.
2) pour tout élément y_2 de F_2, il existe y_1 élément de F_1 tel que $(y_1, y_2) \in R$.

Soit H un ensemble infini de cardinal strictement plus grand que ceux de F_1, F_2.

$H \times R$ s'identifie naturellement à un sous ensemble de $H \times F_1 \times F_2$
$H \times R$ est de même cardinal que H. Soit v_1 (respectivement v_2) une application de $H \times R$ dans F_1 (respectivement F_2) définie de la manière suivante:
3) pour tout élément (h, y_1, y_2) de $H \times R$, $v_1(h, y_1, y_2) = y_1$
4) pour tout élément (h, y_1, y_2) de $H \times R$, $v_2(h, y_1, y_2) = y_2$

D'après (1) et (2) les applications v_1 et v_2 sont des surjections. Le cardinal de H étant infini et strictement plus grand que celui de F_1 et de F_2, les antécédents par v_1 (respectivement par v_2) de tout élément fixé de F_1 (respectivement de F_2) forment un sous-ensemble de $H \times R$ de même cardinal que celui de H.

Soit u_1 (respectivement u_2) une surjection de H dans F_1 (respectivement F_2) telle que pour tout élément de F_1 (respectivement F_2) l'ensemble de ses antécédents par u_1 (respectivement u_2) soit un sous-ensemble de H de même cardinal que celui de H.

Alors d'après l'axiome du choix, il existe des bijections w_1, w_2 de H dans $H \times R$ telles que $u_1 = v_1 \circ w_1$ et $u_2 = v_2 \circ w_2$.
Appelons s la bijection de H dans lui-même définie par $s := w_2^{-1} \circ w_1$.

Un élément quelconque (y_1, y_2) de $F_1 \times F_2$ appartient à R si et seulement si il existe $h \in H$ tel que (h, y_1, y_2) appartienne à $H \times R$.

Autrement dit un élément quelconque (y_1, y_2) appartient à Rsi et seulement si il existe t appartenant à $H \times R$ tel que: $v_1(t) = y_1$ et $v_2(t) = y_2$.

Ce qui est encore équivalent à dire qu'il existe un élément $h \in H$ tel que $v_1(w_1(h)) = y_1$ et $v_2(w_1(h)) = y_2$.

On obtient ainsi qu'un élément quelconque (y_1, y_2) appartient à R si et seulement si il existe $h \in H$ tel que $u_1(h) = y_1$ et $u_2(s(h)) = y_2$. CQFD

8.6.2 Preuve du lemme 169

Soient F_1, F_2 deux ensembles non vides finis. Soit p une une application de $F_1 \times F_2$ dans $[0,_1]$ telle que:

1) la somme des $p(y_1, y_2)$ pour (y_1, y_2) variant dans $F_1 \times F_2$ est 1.

2) p ne prend que des valeurs rationnelles

Soit H un ensemble fini dont le cardinal est multiple de tous les dénominateurs de fractions irréductibles représentant des valeurs prises par p. Soient u_1 (respectivement u_2) une surjection de H dans F_1 (respectivement F_2) avec les propriétés suivantes:

3) pour tout élément y_1 de F_1 le nombre d'antécédents de y_1 par u_1 est le produit de la somme des $p(y_1, w)$ pour w variant dans F_2 et du cardinal de H.

4) pour tout élément y_2 de F_2, le nombre d'antécédents de y_2 par u_2 est égal au produit de la somme des $p(w, y_2)$ pour w variant dans F_1 et du cardinal de H.

Désignons par $card(H)$ le cardinal de H. Construisons alors l'ensemble M défini par:

$$M = \{(k, y, y') \in \times F_1 \times F_2 : 1 \leq k \leq card(H)p(y, y')\}$$

.

Le cardinal de M est égal à celui de H. Soit v_1 (respectivement v_2) une application de M dans F_1(respectivement F_2) définie de la manière suivante:

5) pour tout élément (k, y_1, y_2) de M, $v_1((k, y_1, y_2)) = y_1$

6) pour tout élément (k, y_1, y_2) de M, $v_2((k, y_1, y_2)) = y_2$

On obtient:

7) pour tout élément y_1 de F_1 le nombre d'antécédents de y_1 par u_1 est le produit de la somme des $p(y_1, w)$ pour w variant dans F_2 et du cardinal de H.

8) pour tout élément y_2 de F_2 le nombre d'antécédents de y_2 par u_2 est le produit de la somme des $p(w, y_2)$ pour w variant dans F_1 et du cardinal de H.

Il existe des bijections w_1 et w_2 de H dans M telles que:

$u_1 = v_1 \circ w_1$ et $u_2 = v_2 \circ w_2$. Appelons s la bijection de H dans lui-même définie par:

$$s := w_2^{-1} \circ w_1$$

.

Alors pour tout $(y_1, y_2) \in F_1 \times F_2$, l'ensemble

$$\{h \in H : y_1 = u_1(h) \ et \ y_2 = u_2(s(h))\}$$

est le même que

$$\{h \in H : y_1 = v_1 \circ w_1(h) \ et \ y_2 = v_2 \circ w_1(h))\}$$

.

Comme w_1 est une bijection de H dans M, cet ensemble a le même cardinal que l'ensemble

$$\{m \in M : y_1 = v_1(m) \ et \ y_2 = v_2(m)\}$$

c'est-à-dire que l'ensemble

$$\{(k, y, y') \in \times F_1 \times F_2 : 1 \leq k \leq card(H)p(y_1, y_2) \ et \ y = y_1 \ et \ y' = y_2\}$$

.

Le cardinal l'ensemble $\{h \in H : y_1 = u_1(h) \ et \ y_2 = u_2(s(h))\}$ est donc $card(H)p(y_1, y_2)$. Ceci achève la démonstration du lemme.

Ces lemmes étant acquis, la section qui suit est consacrée aux preuves des théorèmes.

8.7 Preuves des théorèmes 166 et 167

8.7.1 Preuve du théorème 166

On rappelle son énoncé en petits caractères, on veut prouver que :

Les propriétés suivantes sont équivalentes:

- *R est* **fortement non TSD**
- *Il existe un ensemble d'indices non vide I et des applications f_1 (respectivement f_2) de E_1^I dans F_1^I (respectivement de E_2^I dans F_2^I) tel que pour tout élément x de E_1^I et tout élément x de E_2^I, il existe des permutations g_1 et g_2 de I dans lui-même tel que pour tout $i \in I$: $((x(g_1(i)), f1(x_1)(g_1(i))), (x(g_2(i)), f2(x_2)(g_2(i)))) \in R$*

Preuve : Soit $R \subseteq (E_1 \times F_1) \times (E_2 \times F_2)$ telle qu'il existe un ensemble d'indices non vide I et une application f_1 (respectivement f_2) de E_1^I dans F_1^I (respectivement de E_2^I dans F_2^I) avec la propriété suivante:

pour tout élément $x_1 \in E_1^I$ et tout élément $x_2 \in E_2^I$, il existe des permutations g_1, g_2 de I telles que pour tout élément i de I, on a $(x(g_1(i), f_1(x_1)(g_1(i)), x(g_2(i)), f_2(x_2)(g(i))) \in R$.

On veut prouver que R est fortement non TSD.

Considérons la relation 4-aire R' incluse dans $E_1^I \times I \times E_2^I \times I)$ définie comme suit:

un élément (x_1, i_1, x_2, i_2) de $E_1^I \times I \times E_2^I \times I$ appartient à R' quand

$$(x(i_1), f_1(x_1)(i_1), x(i_2), f_2(x_2)(i_2)) \in R$$

Pour tout élément $(x_1, x_2) \in E_1^I \times E_2^I$, il existe des permutations g_1, g_2 de I telles que pour tout $i \in I$:

$$(x_1(g_1(i)), f_1(x_1)(g_1(i)), x_2(g_2(i)), f_2(x_2)(g(i))) \in R$$

.

Pour tout $(x_1, x_2) \in E_1^I \times E_2^I$, il existe des permutations g_1, g_2 de I dans lui-même telles que pour tout élément $i \in I$:

$$(x_1(g_1(g_2^{-1}(i))), f_1(x_1)(g_1(g_2^{-1}(i))), x_2(g_2(g_1^{-1}(i))), f_2(x_2)(g_2(g_1^{-1}(i))))) \in R$$

Par conséquent, pour tout $(x_1, x_2) \in E_1^I \times E_2^I$, et tout élément $i \in I$, il existe des permutations g_1, g_2 de I telles que

$$(x_1, i, x_2, gog_1^{-1}(i)) \in R'$$

Ainsi pour tout $(x_1, x_2) \in E_1^I \times E_2^I$, et tout élément $i \in I$, il existe $i' \in I$ tel que $(x_1, i, x_2, i') \in R'$.

En permutant 1 et 2, on obtient que la relation R' est donc fortement non TSD. Pour montrer que R est fortement non TSD, il suffit de montrer que R se réduit ludiquement à R'.

Fixons un élément i_0 de I.

Soit α_1 (respectivement α_2) l'application de E_1 dans E_1^I (respectivement de E_2 dans E_2^I) qui à un élément x_1 de E_1 (respectivement x_2 de E_2) associe l'unique élément de E_1^I (respectivement de E_2^I) dont toutes les coordonnées sont égales à x_1 (respectivement à x_2).

Soit β_1 (respectivement β_2) l'application de $E_1^I \times I$ dans F_1 (respectivement de $E_2^I \times I$ dans F_2) qui à (x, i) associe $f_1(x)(i)$ (respectivement $f_2(x)(i)$). Par définition de R', pour tout $(x_1, i_1, x_2, i_2) \in E_1 \times I \times E_2 \times I$:

si $(\alpha_1(x_1), i_1, \alpha_2(x_2), i_2) \in R'$, alors $(x_1, \beta_1(x_1, i_1), x_2, \beta_2(x_2, i_2)) \in R$.

Ainsi $R \leq_{lud} R'$ et donc R est fortement non TSD.

Réciproquement

Si R est fortement non TSD alors elle se réduit ludiquement à une relation S incluse dans $A_1 \times B_1 \times A_2 \times B_2$ qui est préfortement non TSD, donc telle que:

1) pour tout élément (x_1, y_1, x_2) de $A_1 \times B_1 \times A_2$, il existe un élément $y_2 \in B_2$ tel que $(x_1, y_1, x_2, y_2) \in S$.

2) pour tout élément (x_2, y_2, x_1) de $A_2 \times B_2 \times A_1$, il existe un élément $y_1 \in B_1$ tel que $(x_2, y_2, x_1, y_1) \in S$.

Soit H un ensemble infini dont le cardinal est strictement supérieur à ceux de B_1, B_2

Soient, pour $i \in \{1; 2\}$, u_i une surjection de H dans B_i telle que pour tout élément de F_i l'ensemble de ses antécédents par u_i soit un sous-ensemble de H de même cardinal que celui de H.

D'après le lemme 9, pour tout couple $(x_1, x_2) \in A_1 \times A_2$, il existe une bijection $s(x_1, x_2)$ de H dans lui-même telle que pour tout couple $(y_1, y_2) \in B_1 \times B_2$, les conditions suivantes sont équivalentes:

- $(x_1, y_1, x_2, y_2) \in S$
- il existe h élément de H tel que:
  3) $y_1 = u_1(h)$ et
  4) $y_2 = u_2(s(x_1, x_2)(h))$

Notons:

$$S' := \{(x_1, h_1, x_2, h_2) \in A_1 \times H \times A_2 \times H \mid h_2 = s(x_1, x_2)(h_1)\}$$

Alors, pour tout élément $(x_1, h_1, x_2, h_2) de A_1 \times H \times A_2 \times H$,

si $(x_1, h_1, x_2, h_2) \in S'$ alors $(x_1, u_1(h_1), x_2, u_2(h_2)) \in S$.
Il s'ensuit $R \leq_{lud} S'$ car $R \leq_{lud} S$ et on vient d'affirmer que $S \leq_{lud} S'$

Il existe alors pour $i \in \{1; 2\}$ une application α_i de $E_i \to A_i$ et une application β_i de $(E_i \times H) \to F_i$ telles que pour tout $(x_1, h_1, x_2, h_2) \in E_1 \times H \times E_2 \times H$:

si $(\alpha_1(x_1), h_1, \alpha_2(x_2), h_2) \in S'$ alors $(x_1, \beta_1(x_1, h_1), x_2, \beta_2(x_2, h_2)) \in R$.

Il s'ensuit que pour tout triplet $(x_1, h, x_2) \in E_1 \times H \times E_2$:

$$(*)\ (x_1, \beta_1(x_1, h), x_2, \beta_2(x_2, s(\alpha_1(x_1), \alpha_2(x_2))(h))) \in R$$

Soit K un ensemble infini de cardinal strictement plus grand que ceux de H, E_1, E_2. Munissons K et H des bons ordres associés leur cardinal.

Munissons alors $K \times H$ de l'ordre lexicographique. Posons $I := K \times H$.

Soit p l'application de I dans K qui à un élément (k, h) de $K \times H$ associe h.

Soit, pour chaque $z \in \{1; 2\}$ l'application γ_z de $E_z^I \times I$ dans I qui à un élément (x, i) de $E_z^I \times I$ associe l'image de i par l'unique isomorphisme de l'ensemble $\{j \in I : x(j) = x(i)\}$ (muni du bon ordre induit par I) dans un segment initial de I.

Soit pour chaque $z \in \{1; 2\}$ l'application f_z de E_z^I dans F_z^I qui à un élément x de E_z^I associe l'application de I dans F_z qui à un élément $i \in I$ associe $\beta_z(x(i), p \circ \gamma_z(x, i))$.

Le cardinal de I est infini et strictement supérieur à celui de H, E_1, E_2. Il s'ensuit que pour tout $(z_1, z_2) \in E_1^I \times E_2^I$:

$$\begin{aligned} &card\{i \in I : card\{j \in I, z_1(j) = z_1(i)\} > card(H)\} \\ =\ &card\{i \in I : card\{j \in I, z_1(j) = z_1(i)\} > card(H)\} \\ =\ &card(I). \end{aligned}$$

Nous pouvons en conclure que pour tout élément $j \in \{1; 2\}$, tout $z_j \in E_j^I$:

$$\begin{aligned} &card\{(x, k) \in E_1 \times K : h \in H, i \in I \gamma_1(z_1, i)(k, h)\ et\ z_1(i) = x\} \\ =\ &card\{(x, k) \in E_2 \times K : h \in H, i \in I \gamma_2(z_2, i) = (k, h)\ et\ z_2(i) = x\} \\ =\ &card(I) \end{aligned}$$

Il s'ensuit que pour tout élément $z_1 \in E_1^I$,tout élément $z_2 \in E_2^I$, et tout $i \in I$:

$$
\begin{aligned}
& card\{j \in I : p \circ \gamma_2(z_2, j) = s(z_1(i), z_2(j))(p \circ \gamma_1(z_1, i))\} \\
&= card\{j \in I : p \circ \gamma_2(z_2, i) = s(z_1(j), z_2(i))(p \circ \gamma_1(z_1, j))\} \\
&= card(I)
\end{aligned}
$$

Par la méthode du va et vient en utilisant le bon ordre sur I on obtient l'existence d'une bijection $S(z_1, z_2)$ de $I \to I$ telle que pour $i \in I$

$$p \circ \gamma_2(z_2, S(z_1, z_2)(i)) = s(z_1(i), z_2(S(z_1, z_2)(i)))(p \circ \gamma_1(z_1, i))$$

D'après (*), nous pouvons en conclure que pour tout élément i de I, $(a, b, c, d) \in R$ en notant:

$a := z_1(i)$,

$b := \beta_1(z_1(i), p \circ \gamma_2(z_2, S(z_1, z_2)(i)))$,

$c := z_2(S(z_1, z_2)(i))$,

$d := \beta_2(z_2(S(z_1, z_2)(i)), s(\alpha_1(z_1(i)), \alpha_2(z_2(S(z_1, z_2)(i)))(p \circ \gamma_1(z_1, i)))))$

Cela signifie que pour tout élément $i \in I$:

$$(z_1(i), f_1(z_1)(i), z_2(S(z_1, z_2)(i)), f_2(z_2)(S(z_1, z_2)(i))) \in R$$

ce qui achève la démonstration du théorème 166.

8.7.2 Preuve du théorème 167

On rappelle son énoncé en petits caractères, on veut prouver que :

Les propriétés suivantes sont équivalentes:

- *R est* **casino-inoffensif**
- *Il existe un ensemble* **fini** *d'indices non vide I et des applications f_1 (respectivement f_2) de E_1 dans F_1^I (respectivement de E_2 dans F_2^I) tel que pour tout élément x_1 de E_1 et tout élément x_2 de E_2, il existe des permutations g_1 et g_2 de I dans lui-même tel que pour tout $i \in I$: $((x_1, f_1(x_1)(g_1(i))), (x_2, f_2(x_2)(g_2(i)))) \in R$*

Preuve : On suppose ici E_1, F_1, E_2, F_2 **finis** et R une garantie telle qu'il existe un ensemble d'indices fini non vide I et des applications f_1, f_2 de E_1 dans F_1^I (respectivement de E_2 dans F_2^I) tel que pour tout $x_1 \in E_1$ et tout $x_2 \in E_2$, il existe des permutations g_1 et g_2 de I dans lui-même tel que pour tout $i \in I$:

$$(x_1, f_1(x_1)(g_1(i)), x_2, f_2(x_2)(g_2(i))) \in R$$

.

Bien que g_1, g_2 dépendent de (x_1, x_2), on conserve cette notation pour ne pas alourdir l'écriture.

Soit p l'application de $E_1 \times F_1 \times E_2 \times F_2 \to [0,_1]$ qui à (x_1, y_1, x_2, y_2) associe le quotient

$$\frac{card(\{i \in I : y_1 = f_1(x_1)(g_1(i)) \ et \ y_2 = f_2(x_2)(g_2(i))\})}{card(I)}$$

pour tout couple (x_1, x_2) de $E_1 \times E_2$, la somme des $p(x_1, y, x_2, y')$ pour (y, y') variant dans $F_1 \times F_2$ est égale à 1.

Par changement de variable en remplaçant i par $g_1^{-1}(i)$, on obtient:

$$p(x_1, y_1, x_2, y_2) = \frac{card(\{i \in I : y_1 = f_1(x_1)(i) \ et \ y_2 = f_2(x_2)(g_2(g_1^{-1}(i)))\})}{card(I)}$$

La somme des $p(x_1, y_1, x_2, y)$ pour y variant dans F_2 est alors égale à:

$$\frac{card(\{i \in I : y_1 = f_1(x_1)(i)\})}{card(I)}$$

résultat qui ne dépend que de (x_1, y_1).

En permutant les indices 1 et 2, on arrive à la conclusion similaire que la somme des $p(x_1, y, x_2, y_2)$ pour y variant dans F_1 vaut:

$$\frac{card(\{i \in I : y_2 = f_2(x_2)(i)\})}{card(I)}$$

résultat qui ne dépend que de (x_2, y_2).

Conclusion: R est casino-inoffensive

Réciproquement

Supposons R casino-inoffensive. Il existe alors une application p dans $E_1 \times F_1 \times E_2 \times F_2 \rightarrow [0,_1]$ telle que:

1) Pour tout couple (x_1, x_2) de $E_1 \times E_2$, la somme des $p(x_1, x_2, y_1, y_2)$ pour (y_1, y_2) variant dans $F_1 \times F_2$ est égale à 1.

2) Pour un triplet (x_1, y_1, x_2) de $E_1 \times F_1 \times E_2$,la somme des $p(x_1, y_1, x_2, y)$ pour y variant dans F_2 ,ne dépend que de x_1, y_1 , la propriété restant vérifiée si on permute les indices 1 et 2.

3) Pour tout quadruplet (x_1, x_2, y_1, y_2) de $E_1 \times F_1 \times E_2 \times F_2$ tel que $p(x_1, y_1, x_2, y_2) \neq 0$, on a $(x_1, y_1, x_2, y_2) \in R$.

L'existence de p revient donc à l'existence d'une solution réelle pour un système fini (car les ensembles considérés sont finis) d'équations et d'inéquations linéaires à coefficients rationnels.

Or pour un système fini d'équations et d'inéquations linéaires à coefficients rationnels, il existe une solution rationnelle si et seulement si il existe une solution réelle.

Nous pouvons donc sans perte de généralité supposer que p ne prend que des valeurs rationnelles.

Soit I un ensemble fini dont le cardinal est multiple de tous les dénominateurs de fractions irréductibles représentant des valeurs prises par p.

Soit (x_1, x_2) un couple de $E_1 \times E_2$. Soient $u_1(x_1, x_2)$ (respectivement $u_2(x_1, x_2)$) une application de H dans F_1 (respectivement F_2) avec les propriétés suivantes:

4) pour tout élément $y_1 \in F_1$ le nombre d'antécédents de y_1 par $u_1(x_1, x_2)$ est le produit de la somme des $p(x_1, y_1, x_2, w)$ pour w variant dans F_2 par le cardinal de H.

5) pour tout élément $y_2 \in F_2$ le nombre d'antécédents de y_2 par $u_2(x_1, x_2)$ est le produit de la somme des $p(x_1, w, x_2, y_2)$ pour $u_2(x_1, x_2)$ variant dans F_1 et du cardinal de H.

Comme d'après (2) la première somme considérée ne dépend que de (x_1, y_1) et la deuxième somme ne dépend que de x_2, y_2, on peut imposer à $u_1(x_1, x_2)$ de ne dépendre que de x_1 et à $u_2(x_1, x_2)$ de ne dépendre que de x_2.

Dorénavant on notera ces applications $u_1(x_1)$ et $u_2(x_2)$.

D'après le lemme2, il existe une bijection $s(x_1, x_2)$ de H dans lui-même telle que pour tout élément $(y_1, y_2) \in F_1 \times F_2$, $p(x_1, x_2, y_1, y_2)$ est:

$$\frac{card(\{h \in H : y_1 = u_1(x_1)(h) \ et \ y_2 = u_2(x_2)(s(x_1, x_2)(h))\})}{card(H)}$$

.

Il s'ensuit que pour tout élément h de H, $p(x_1, u_1(x_1)(h), x_2, u_2(x_2)(s(x_1, x_2)(h))) \neq 0$.

Donc pour tout élément h de H, $(x_1, u_1(x_1)(h), x_2, u_2(x_2)(s(x_1, x_2)(h))) \in R$.

Il suffit alors de poser $I := H, f_1 := u_1, f_2 := u_2, g_1 := Id, g_2 := s(x_1, x_2)$ pour obtenir la conclusion cherchée.

8.8 Remarque sur les différences entre les deux théorèmes

Le résultat du deuxième théorème n'est pas exactement l'équivalent casino-inoffensif de ce que le premier théorème est pour les fortement non TSD. Si on adaptait la démonstration du premier théorème, on obtiendrait seulement:

Une garantie est casino inoffensive si et seulement pour tout $\epsilon > 0$, il existe un ensemble d'indices non vide I fini et des applications $f_1 f_2$ tels que pour tout (x_1, x_2), il existe des permutations g_1, g_2 de I tel que pour une proportion d' éléments i de I supérieure à $1 - \epsilon$:

$$(x_1(g_1(i)), f_1(x_1)(g_1(i)), x_2(g_2(i)), f_2(x_2)(g(i))) \in R$$

Comme nous allons le voir dans le contre-exemple qui suit, il existe une garantie casino-inoffensive qui ne vérifie pas la conclusion idéalisée où on remplacerait ϵ par 0.

8.8.1 Contre-exemple

Posons $E_1 := F_1 := E_2 := F_2 := \{0; 1\}$. On considèrera au cours du raisonnement que 2 est muni de sa structure canonique de corps à deux éléments.

Soit R la garantie dont les éléments sont les quadruplets $(x_1, y_1, x_2, y_2) \in E_1 \times F_1 \times E_2 \times F_2$ tels que:

$$y_1 + y_2 = x_1 x_2$$

Alors R est casino-inoffensive. Il suffit de définir p de la manière suivante:

pour tout quadruplet (x_1, y_1, x_2, y_2) de $E_1 \times F_1 \times E_2 \times F_2$:
$p(x_1, y_1, x_2, y_2) := 0,5$ si $(x_1, y_1, x_2, y_2) \in R$
$p(x_1, y_1, x_2, y_2) := 0$ si $(x_1, y_1, x_2, y_2) \notin R$

Théorème 170 *R n'est pas fini-multi-permut-all-table*

Nous verrons à la fin du chapitre que *tous les téléphones quantiques sont fini-mutli-permut-table.* Cela les différencie donc des casino-inoffensifs.

Preuve : Supposons qu' il existe un ensemble d'indices non vide I fini et, pour chaque $k \in \{1;2\}$ une application f_k de E_k^I dans F_k^I telle que pour tout $(x_1, x_2) \in E_1^I \times E_2^I$, il existe des permutations g_1, g_2 de I tel que pour tout élément i de I

$$(x_1(g_1(i)), f_1(x_1)(g_1(i)), x_2(g_2(i)), f_2(x_2)(g(i))) \in R$$

.

Quitte à remplacer I par $I \times \{0,1\}$ et g_k par l'application qui à chaque $(i,j) \in I \times 2$ associe $(g_k(i), j)$, on peut sans perte de généralité, supposer que le cardinal de I est pair.

Comme ici F_1, F_2 sont égaux à 2 , on peut définir l' application s_k de E_k^I dans 2 qui à un élément x de E_k^I associe la somme pour i variant dans I des $f_k(x)(i)$

Soit a l'élément de 2^I tel que $\forall i \in I : a(i) = 1$

Soit b l'élément de 2^I tel que $\forall i \in I : a(i) = 0$

Soit c un élément de 2^I tel que $a(i) = 1$ pour un et un seul élément i de I.

Comme pour tout élément $i \in I$ et tout $(x_1, x_2) \in E_1^I \times E_2^I$, il existe des permutations g_1, g_2 de I telles que pour tout $i \in I$:

$$(x(g_1(i)), f_1(x_1)(g_1(i)), x(g_2(i)), f_2(x_2)(g(i))) \in R$$

On obtient alors pour tous $(i, x_1, x_2) \in I \times E_1^I \times E_2^I$:

$$f_1(x_1)(g_1(i)) + f_2(x_2)(g_2(i)) = x_1(g_1(i))x_2(g_2(i))$$

Par sommation de l'égalité ci-dessus sur i variant dans I, utilisation de la puplicité du cardinal de I et remplacement de x_1, x_2 par a, b ou c, on obtient les relations suivantes:

$s_1(a) + s_2(a) = 0$ donc $s_1(a) = s_2(a)$

$s_1(a) + s_2(b) = 0$ donc $s_1(a) = s_2(b)$

$s_1(b) + s_2(a) = 0$ donc $s_1(b) = s_2(a)$

$s_1(b) + s_2(b) = 0$ donc $s_1(b) = s_2(b)$

$s_1(c) + s_2(b) = 0$ donc $s_1(c) = s_2(b)$

$s_1(b) + s_2(c) = 0$ donc $s_1(b) = s_2(c)$

$s_1(a) + s_2(c) = 1$ donc $s_1(a)s_2(c)$

$s_1(c) + s_2(a) = 1$ donc $s_1(c)s_2(a)$

Pour les relations qui nous intéressent, le résultat ne dépend pas du choix de (g_1, g_2).

Les 6 premières égalités entraînent que $s_1(a), s_2(a), s_1(b), s_2(b), s_1(c), s_2(c)$ sont tous égaux, ce qui est contredit par les deux dernières inégalités. Nous avons donc une contradiction

Dans la section suivante, on établit qu'un téléphone T **qui n'est pas** casino-inoffensif permet à un couple Alice-Bob de fomenter une stratégie lui permettant d'augmenter son espérance de gain au *jeu du casino surveillé par T.*

8.9 Motivation du terme *casino-inoffensif*

Nous allons retenir une version plus symétrique de jeu surveillé par T que celle décrite au début du chapitre.

8.9.1 Description du jeu étudié, choix d'un protocole

Pour fixer les idées, Alice est sur Terre et Bob est sur Mars. Ils n'ont aucun moyen de communication entre eux, sauf des boîtiers avec des boutons et des lampes. Dans cette version leur rôle va être symétrique. Comme dit enintroduction, une mathématisation du sens unique parait inaccesible

Chaque joueur dispose d'un et un seul boîtier. Lorsqu'un joueur appuie sur un bouton, il s'allume une lampe et une seule.

Le casino à le pouvoir de faire allumer les lampes qu'il veut, autrement dit, en fait **le casiono simule le téléphone**.

On dispose de deux ensembles finis ou dénombrables N_1, N_2 de nombres (qui ont chacun au moins 2 éléments).

Le casino **tire au hasard** un nombre dans N_1 qu'il montre à Alice et un nombre dans N_2 qu'il montre à Bob.

Le but de chacun est de parier sur le nombre qu'a reçu l'autre: il gagne une certaine somme d'argent si sa réponse est correcte, et en perd sinon.

Les tirages sont organisés de telle façon que, pour chaque joueur, l'espérance de gain soit la même quelque soit le choix qu'il fait (si les deux tirages de nombres sont supposés correlés on remplace espérance de gain par espérance de gain sachant le nombre que l'on a reçu).

Appelons E_1 l'ensemble des boutons du clavier d'Alice et F_1 l'ensemble des lampes de ce même boîtier. De même, avec l'indice 2 au lieu de 11, en ce qui concerne Bob.

Soit R une garantie incluse dans $E_1 \times F_1 \times E_2 \times F_2$. Le jeu se déroule de la manière suivante.

Une fois les tirages effectués et que les joueurs ont vu leur nombre, le casino demande au deux joueurs d'appuyer simultanément sur un bouton de leur boîtier c'est-à-dire au moment où le casino leur aura donné le signal.

Quand Alice a appuyé un bouton x_1 et que Bob a appuyé un bouton x_2, le casino choisit d'allumer une lampe y_1 sur le premier boitier et une lampe y_2 sur le deuxième boîtier. **Le casino fait ce choix librement, et il n'a aucune contrainte de recourir à une démarche aléatoire**.

La seule contrainte que la casino doit respecter est que $(x_1, y_1, x_2, y_2) \in R$: on dit que le système des deux boîtiers est $R-garanti$ par le casino. Ce n'est qu'après avoir vu leur lampe s'allumer que chacun des deux essayera de deviner le nombre reçu par l'autre.

Les théorèmes qui suivent établissent l'équivalence entre la définition technique et la notion souhaité de *"casino-inoffensivité"*.

Le dernier théorème situe la classe des téléphones à deux combinés FMQ par rapport à la notion de casino-inoffensivité. Tous les FMQ sont casino-inoffensifs. Par contre, il existe des casino-inoffensifs qui ne sont pas FMQ, et le contre-exemple de la sous-section précédente en est un témoin.

Théorème 171 *On suppose F_1, F_2 finis. Si R n'est pas casino-inoffensive, quelque soit la stratégie employée par le casino, l'équipe des deux joueurs a une stratégie pour obtenir une espérance de gain meilleure que si le système des boîtiers n'existait pas.*

Preuve :

Supposons qu'il existe une stratégie pour le casino telle que quelque soit la stratégie employée par l'équipe des deux joueurs, il ne peuvent obtenir une espérance de gain meilleure que ce qu'ils auraient pu obtenir si le système des boîtiers n'existait pas.

Supposons qu'Alice et Bob se mettent d'accord sur la stratégie suivante: ils décident qu'Alice appuie sur le bouton x_1 et que Bob appuie sur le bouton x_2 et ce indépendemment des nombres qu'on leur montrera.

Dans ce cas la probabilité d'allumage d'une lampe y_1 dans le boitier d'Alice ne dépend que du nombre qu'on lui a montré. Sinon, d'après la formule de Bayes, les probabilités conditionnelles sachant y_1 des nombres montrés à Bob dépendraient de y_1.

On aurait alors nécessairement au moins un y_1 et un nombre n_2 montré à Bob telle que sa probabilité d'être tiré sachant que la lampe y_1 s'est allumée soit supérieure à sa probabilité d'être tiré sans le savoir.

Les espérances " à priori " de tirages des nombres montrés à Bob étant égales, en misant sur n_2, Alice pourrait alors obtenir une espérance de gain supérieure à celle qu'elle aurait obtenue si le système de boîtiers n'existait pas (stratégie passive en quelque sorte).

Supposons maintenant que Bob fasse dépendre le bouton x_2 qu'il appuie du nombre que le casino lui montre (stratégie en quelque sorte active).

Par le même raisonnement que précédemment, la probabilité d'allumage d'une lampe y_1 dans le boîtier d'Alice ne dépend que du nombre qu'on lui a montré.

De tout cela nous pouvons déduire que si (n_1, n_2) est un couple fixé de $N_1 \times N_2$ (l'égalité des espérances de gain entraîne que la probabilité du tirage de (n_1, n_2) est non nulle), alors la probabilité que la lampe y_1 s'allume dans le boîtier d'Alice ne dépend que de x_1.

Alors soit $p(x_1, y_1, x_2, y_2)$ la probabilité que la lampe y_1 du boîtier d'Alice et la lampe y_2 du boîtier de Bob s'allument si Alice a appuyé sur le bouton x_1 et que Bob a appuyé sur le bouton x_2.

On obtient alors que la somme des $p(x_1, y_1, x_2, y)$, y parcourant F_2 ne dépend que de x_1. Par le même raisonnement, on a le même résultat en échangeant Alice et Bob.

La probabilité p est une application de $E_1 \times F_1 \times E_2 \times F_2$ dans $[0, 1]$ telle que pour tout couple $(x_1, x_2) \in E_1 \times E_2$, la somme des $p(x_1, x_2, y_1, y_2)$ pour (y_1, y_2) variant dans $F_1 \times F_2$ est égale à 1.

Le fait que le système de boîtiers soit " R-garanti " entraîne que pour tout quadruplet $(x_1, x_2, y_1, y_2) \in E_1 \times E_2 \times F_1 \times F_2$, si $p(x_1, x_2, y_1, y_2) \neq 0$ alors $((x_1, y_1), (x_2, y_2)) \in R$.

La relation R est alors casino-inoffensive.

Le théorème suivant est la réciproque du précédent:

8.9.2 Un degré casino-inoffensif n'avantage pas au casino

Théorème 172 *On enlève l'hypothèse d'égalité des espérances. Si la relation R est casino-inoffensive, alors le casino a une stratégie telle que quelque soit la stratégie employée par l'équipe des deux joueurs, il ne peuvent obtenir une espérance de gain meilleure que ce qu'ils auraient pu obtenir si le système des boîtiers n'existait pas.*

Preuve :

On suppose R casino-inoffensive, on reprend exactement les mêmes noms pour la probabilité, etc, et le même énoncé que pour l'énoncé des propriétés listée dans la définition de casino-inoffensivité:

1. Pour tout couple $(x_1, x_2) \in E_1 \times E_2$, la somme des $p(x_1, x_2, y_1, y_2)$ quand y varie dans $F_1 \times F_2$ est égale à 1.
2. Pour un triplet (x_1, y_1, x_2), la somme des $p(x_1, x_2, y_1, y_2)$, y_2 variant dans F_2 ne dépend que du couple (x_1, y_1) , la propriété restant vérifiée si on permute les indices 1 et 2.
3. Pour tout quadruplet q si $p(q) \neq 0$ alors $q \in R$

Le casino peut utiliser la stratégie suivante:

Si Alice appuye sur le bouton x_1 et que Bob appuye sur le bouton x_2, alors le casino allume la lampe y_1 dans le boîtier d'Alice et la lampe y_2 dans le boîtier de Bob avec la probabilité $p(x_1, x_2, y_1, y_2)$ indépendemment des tirages effectués. Cette stratégie est licite car compatible avec le fait que le système de boîtiers soit R-garanti.

Par les mêmes raisonnements que pour le théorème précédent, on obtient que la probabilité d'allumage de la lampe y_1 ne dépend que de x_1, et ceci indépendemment des stratégies utilisées par l'équipe Alice-Bob.

En réutilisant la formule de Bayes, on obtient que les probabilités de tirage du nombre montré à Bob sachant que la lampe y_1 s'est allumée sont les mêmes que ne le sachant pas.

Il s'ensuit que les espérances de gain pour Alice sachant que la lampe y_1 s'est allumée sont les mêmes que ne le sachant pas. Par le même raisonnement, c'est également vrai pour Bob. Ce qui achève la démonstration du théorème 13.

8.10 Téléphones quantiques réels. Puissance?

Nous utilisons dans cette section la définition suivante pour les téléphones à deux combinés.

Définition 173 *Soit E un espace hermitien de dimension finie k. Soient $E_1 := E_2 :=$ l'ensemble des bases orthonormées de E. Soit A une forme bilinéaire non nulle sur E.*

Si b est une base de E, on note $b(i)$ son ième élément. Soit $R(A, E)$ la relation:

$$R(A, E) := \{((u, i), (v, j)) \in E_1 \times F_1 \times E_2 \times F_2 \mid A(u(i), v(j)) \neq 0\}$$

Les relations FMQ sont par définition celles S telles qu'il existe un espace hermitien de dimension finie E et une forme bilinéaire non nulle A sur E tels que $S \leq_{lud} R(A, E)$

On remarque que le fait qu'une garantie soit oui ou non FMQ ne dépend par définition que de son degré ludique. Le théorème suivant énonce que les degrés FMQ sont finimultipermutalltable. *Rappel: cette propriété se décrit avec un simple copié-collé de celle qui caractérise les fortement nonTSD en ajoutant le mot* **fini** *pour le nombre de tables sur lesquelles on joue*

Théorème 174 *Soit R une garantie FMQ, telle que ses claviers et écrans sont tous finis. Alors:*

Il existe un ensemble FINI I d'indices non vide et des applications f_1 (respectivement f_2) de E_1^I dans F_1^I (respectivement de E_2^I dans F_2^I) tel que pour tout élément x de E_1^I et tout élément x de E_2^I, il existe des permutations g_1 et g_2 de I dans lui-même tel que pour tout $i \in I$:

$$((x(g_1(i)), f1(x_1)(g_1(i))), (x(g_2(i)), f2(x_2)(g_2(i)))) \in R$$

Preuve :

Il est facile de voir que la garantie ne dépend que du degré ludique. Soit $R(A, E)$ une relation FMQ et r le rang de la forme bilinéaire A. Posons $I := \{1, 2, \ldots, r\}$. La forme bilinéaire A étant définie sur l'espace hermitien E, il existe une application linéaire unique $T \in L(E, E)$ telle que, pour tout couple (u, v) de vecteurs de $E :< T(u), v >= A(u, v)$.

Soit T^* l'adjoint de T. Définissons, pour $w \in \{1; 2\}$ l'application f_w de E_w^I dans F_w^I de la manière suivante. On convient que T_1 signifie T et que T_2 signifie T^*.

A un r-uplet $(b_1, , b_r)$ de bases orthonormées de E, on associe le r-uplet d'entiers $(k_1, , k_r)$ où k_1 est le plus petit des indices k tel que:

$$T_w(b_1(k)) \neq 0$$

, et, pour tout entier $s \in \{1, 2, , r\}$, k_s est le plus petit indice k tel que la famille:

$$(T_w(b_1(k_1)), T_w(b_2(k_2)), T_w(b_{s-1}(k_{s-1})), T_w(b_s(k)))$$

soit libre.

D'après le théorème de la base incomplète un tel r-uplet d'entiers existe bien.

Soit $x_1 = (b_1 \ldots, b_r)$ et $x_c := (c_1, \ldots, c_r)$ deux r-uples de bases orthonormées de E. Considérons alors la matrice M d'ordre r définie de la manière suivante:

$$M(i, j) := A(x_1(i)(f_1(x_1)(i)), (x_2(j)(f_2(x_2)(j))))$$

La matrice M est inversible. Son déterminant est donc non nul. Il existe donc une permutation $s(x_1, x_2)$ de I tel que pour pour tout élément $i \in I$:

$$A(x_1(i)(f_1(x_1)(i)), x_2(s(x_1, x_2)(i))(f_2(x_2)(s(x_1, x_2)(i)))) \neq 0$$

C'est à dire,

$$(x_1(i), f_1(x_1)(i), x_2(s(x_1, x_2)(i)), f_2(x_2)(s(x_1, x_2)(i))) \in R$$

Il suffit alors de poser $g_1 = Id$ et $g_2 = s(x_1, x_2)$ pour obtenir la conclusion désirée.

Chapitre 9

En guise de conclusion. Hasard ou convenance?

On aura noté que les innombrables preuves que la théorie quantique prédit une nature obligatoirement indéterministe sont en fait des preuves qui ne parle à aucun moment de "hasard". Des modifications de ces preuves conduisent tout autant à des conclusions encore plus édifiantes: impossibilité de cloner, pied de nez de la non localité quantique face au dogme relativiste d'impossibilité d'envoyer "un bit" plus vite que la lumière, etc.

En fait, **même en acceptant** de calculer des probabilités, force est de constater que **que c'est parce que les statistiques** prédites par la théorie quantique changent que nous avons pu la distinguer d'un théorie "classique" où le hasard ne survient que comme commodité notationnelle pour contourner l'ignorance de réalités supposées banales. La section suivante invalide un préjugé qui voudrait qu'à statistiques égales une théorie ne puisse s'avérer franchement et reproductiblement indéterministe. Une autre manière d'énoncer ce préjugé est de dire que *tant que les statistiques se conforment aux prévisions de la théorie classique des probabilités mathématiques des manuels, il n'y a aucun moyen de distinguer entre l'ignorance des conditions initiales polluantes (le bruit classique) et un aléa réel de la nature.*

9.1 Distinction clinique du vrai hasard à constats statistiques égaux

Dans cette section, nous montrons que sur le plan des principes mathématiques, *sans aucun viol* de probabilités "classiques", il existe un protocole qui permet de distinguer si un état est déterminé avant d'être regardé ou si la demande de l'information, fut-elle de principe, par les spectateurs produit un tirage aléatoire qui le sélectionne. On utilise l'axiome du choix.

9.1.1 Le jeu

Soit E un ensemble contenant au moins deux éléments et Z un ensemble infini. Bob remplit (ou non) des boites numérotée par Z avec des éléments d'un ensemble E. Autrement dit, il choisit (ou non) un élément de f de E^Z.

Alice peut ouvrir certaines boites, mais pas toutes. Par *ouvrir*, on entend qu'elle choisit un ensemble Y_1 inclus dans Z et Bob l'informe du contenu des boites dont les numéros sont dans Y_1, autrement dit il montre à Alice un élément de E^{Y_1} (qui est censé être la restriction de f à Y_1). Après quoi, Alice peut recommencer, avec un Y_2 de son choix. Puis enfin elle choisit une boite *qu'elle n'a pas ouverte*, c'est-à-dire dont le numéro n'est pas un élément de $Y_1 \cup Y_2$. Désignons son numéro par $i \in Z$. Elle doit alors parier sur son contenu.

Par *parier*, on entend proposer un élément x de E. Bob révèle alors à Alice la valeur $f(i)$ de la boite et Alice gagne si $x = f(i)$

Il est évident que si Bob triche, c'est à dire ne choisit pas une $f \in E^Z$ avant que commence la partie, il n'a pas de mal à gagner. Mais le protocole interdit à Alice d'ouvrir les boites d'une manière directe ou indirecte pour vérifier que Bob ne triche pas.

La question est donc de se demander s'il existe une façon de procéder, quand on est Alice, pour *s'apercevoir* que Bob triche. Le préjugé disons le plus répandu voudrait que non. Il se trouve, que sans faire la moindre référence à une quelconque nature quantique ou à une quelconque magie, la réponse est quand-même oui et atteste que vrai hasard et ignorance des conditions initiales sont *sur le principe* "cliniquement" discernables en un sens qui va apparaître dans ce qui suit.

9.1.2 Stratégie pour Alice

Dans cette section, on suppose que *Bob ne triche pas*, i.e. il remplit bien les boites avant que la partie démarre (Il les remplit comme il veut, mais il les remplit).

Soit n un entier. Nous décrivons une famille de n stratégies $s_0, .., s_{n-1}$ ayant la propriété suivante: pour toute $f \in E^Z$ (remplissage choisi par Bob), il existe $i \in n$ tel que pour tout $j \in n \setminus \{i\}$, Alice gagne en suivant la stratégie s_j quand Bob a rempli les boites avec f. Rappelons qu'on n'est pas dans le "fini". Pour cela Alice doit disposer d'une fonction ϕ de Galvin sur E. Nous rappelons donc la définition d'une fonction de Galvin et le théorème d'existence donnée au Chapitre 6 et nous donnons une démonstration. Rappelons d'abord ce qu'est la fonction S (Shift) de $E^{\mathbb{N}}$ dans $E^{\mathbb{N}}$. Elle est définie, pour $u \in E^{\mathbb{N}}$ par la formule:

$$\forall n \in \mathbb{N},\ S(u)_n = u_{n+1}.$$

Définition 175 *On dit que ϕ est une fonction de Galvin de E si c'est une application de $E^{\mathbb{N}}$ dans E qui vérifie la relation:*

$$\forall u \in E^{\mathbb{N}},\ \exists p \in \mathbb{N} : \forall n \geq p,\ u_n = \phi(S^{n+1}(u)).$$

Théorème 176 *Soit E un ensemble. Il existe une fonction de Galvin, ϕ sur E, Le premier entier p vérifiant la propriété ci-dessus sera notée score(u)*

Preuve :

Soit r un bon ordre sur $E^{\mathbb{N}}$. Soit $u \in E^{\mathbb{N}}$. si u est périodique de période principale p, on définit $\phi(u) := u(p-1)$. Sinon, on définit la fonction $\psi : E^{\mathbb{N}} \to E^{\mathbb{N}}$ par la formule : $\psi(u) := min_r(\{v \in E^{\mathbb{N}} \mid \exists k(u,v) \in \mathbb{N} : u = S^{k(u,v)}(v)\})$ et $\phi(u) := \psi(u)(k(u, \psi(u)))$. On vient de définir une application de $E^{\mathbb{N}} \to E$.

Soit $u \in E^{\mathbb{N}}$. On peut la supposer non périodique. Quitte à la remplacer par $S^q(u)$ avec q assez grand, on peut supposer que $\forall n \in \mathbb{N},\ \psi(S^n(u)) = \psi(u)$. En effet, la suite $n \mapsto \psi(S^n(u))$ de $(\mathbb{N}, \leq)$ dans $(E^{\mathbb{N}}, r))$ est clairement décroissante, donc stationnaire car r est un bon ordre. Dès lors, on constate que $\forall n \in \mathbb{N} : \phi(S^{n+1}(u)) = u_n$.

Sans perte de généralité, on suppose que $Z = \mathbb{N} \times n$. On se donne une fonction ϕ de Galvin sur E.

Description de la stratégie s_i

Alice demande à Bob de lui révéler le contenu de toutes les boites dont le numéro est un élément de la forme (q, j) avec $q \in \mathbb{N},\ j \neq i$. Pour chaque $k \in n \setminus \{i\}$, elle calcule alors $e_k := score(q \mapsto f(q, k))$.

Puis elle calcule $r := 1 + max_i e_i$. Elle demande alors à Bob d'ouvrir les boites dont les numéros sont (q, i) avec $q > r$. On remarque que les boites restées fermées sont les numéros (p, i) tels que $p \leq r$.

Elle calcule $v := \phi(p \mapsto f(r + 1 + p, i)$. Et enfin, elle parie sur v.

9.1.3 Théorème

Il est facile de vérifier que

Lemme 177 *La stratégie s_i échoue seulement si pour tout $j \in n \setminus \{i\}$: $score(p \mapsto f(p, i)) > score(p \mapsto f(p, j))$*

Il s'ensuit que:

Théorème 178 *Pour toute $f \in E^Z$ (remplissage choisi par Bob), il existe $i \in n$ tel que, pour tout $j \in n \setminus \{i\}$, Alice gagne en suivant la stratégie s_j quand Bob a rempli les boites avec f*

9.1.4 Bob triche-t-il

Si on remplace un choix par Bob de $f \in E^Z$ fait avant la partie par un tirage au sort ou tout autre procédure qui décide du contenu des boites ouvertes au moment où on les ouvre, Alice ne peut plus espérer avoir $n-1$ chances sur n de gagner comme à la section précédente.

Si on était des géants, (i.e. si on pouvait jouer avec des ensembles infinis), on aurait un procédé falsifiable (moyennant certes l'axiome du choix) pour savoir si le contenu de boites fermées, qu'on ouvre, étaient déjà déterminés avant qu'on ne décide de les ouvrir. Pour le faire, nous n'avons eu recours à aucun argument d'inspiration quantique

Bibliographie

[Ba] T. Bartoszynski, Additivity of measure implies additivity of category, *Trans. Amer. Math. Soc.*, vol.*281* (1984), pp. 209-213

[B.S.] T. Bartoszynski and S. Shelah, Closed measure zero sets, *Annals of Pure and Applied Logic*, vol.*52* (1992), pp. 93-110

[Can] Journal canadien sur la theorie des graphes 1996

[Car] Bartoszinski. Combinatorial aspect of measure and category. Fund Math 127 (1987) 225-239

[Cha1] C. Chalons, Degrés ludiques, 1999, prépublication

[Cha2] C. Chalons, A unique integer associated to each map from E^ω to ω, C.R.A.S., Série I Mathématiques 331 (2000), p. 501.

[Cha3] C. Chalons, Degrés ludiques et Jeux, 2012, prépublication.

[Cha4] C. Chalons,The Target's theorem, article en cours de publication sur HAL (2014).

[Cha5] C. Chalons, L'effacement du temps par les anneaux commutatifs, article en cours de publication sur HAL (2014).

[C.R.] C. Chalons et J.P. Ressayre, Degres Ludiques, New Studies in Weak Arithmetics, September 2013

[Da] M.M. Day, Oriented Systems, Duke Math. Journal, vol.*11* (1944), pp.201-229

[Del] J.P. Delahaye,Libre arbitre et mécanique quantique, LOGIQUE et CALCUL, 2009

[D.R.] Diener et Reeb: Analyse non standard.

[Esp] Bernard D'espagnat: Le réel voilé. Paris Fayard 1994

[Eve] Voir chapitre 12 de [Esp]

[E.V.] A. C. Elitzur and L. Vaidman, Quantum mechanical interaction-free measurements, Found. Phys. 23, 1993, 987-97.

[Fr1] D.H. Fremlin, The partially ordered sets of measure theory and Tukey's ordering, *Note di Matematica*, vol.*XI* (1991), pp. 177-214

[Fr2] D.H. Fremlin, Families of compact sets and Tukey's ordering, *Atti Sem. Mat. Fis. Univ. Modena*, vol.*XXXIX* (1990), pp. 29-50

[Fr3] D.H. Fremlin, *Problems*, version of 3 January 1996

[G.I.] S. Ginsburg and J.R. Isbell, The category of cofinal types, I, *Trans. Amer. Math. Soc.*, vol.*116* (1965), pp. 386-393

[G.P.] F. Galvin and K. Prikry, Infinitary Jonsson algebras and partition relations, *Algebra Universalis*, vol.*6* (1976) 367-376

[Is1] J.R. Isbell, The category of cofinal types, II, *Trans. Amer. Math. Soc.*, vol.*116* (1965), pp. 384-416

[Is2] J.R. Isbell, "Seven cofinal types", *J. London Math. Soc.(2)*, vol.*4* (1972), pp. 651-654

[Kan] Kanamori: Higher infinite springer verlag 1994

[Kec] A. Kechris, *Classical Descriptive Set Theory*, Springer-Verlag, 1995

[Khe] A. Khélif, Degrés inoffensifs et degrés FMQ, 2012, prépublication.

[Kri] Krivine:λ-calcul type et modèle. Paris Masson 1990

[Kun] Kunen 1980: Set Theory. Springer verlag

[Pen] Roger Penrose: Les ombres de l'esprit. traduction de Shadows of mind. Paris interéditions 1995

[Pra] Pratt every prime has a succint certificate SIAM journal on computing Vol 4 214-252 Theory of ultrafilters. Comfort Negrepontis Springer Verlag 1974

[Tod1] S. Todorcevic, Directed sets and cofinal types, *Trans. Amer. Math. Soc.*, vol.*290* (1985), pp. 711-723

[Tod2] S. Todorcevic, A classification of transitive relations on $\aleph_1$, *Proc. London Math. Soc.*, vol.*73(3)*, (1996), pp. 501-533

[Tuk] J.W. Tukey, *Convergence and Uniformity in Topology*, Princeton University Press 1940

[Voj] P. Vojtáš, "Generalized Galois-Tukey connections between explicit relations on classical objects of real analysis", *Israel Math. Conference Proceedings*, ed. H. Judah, vol.*6*, (1991), pp. 619-643

[YIPARAKI] On some partition propertie, PhD thesis University of Michigan, 1994.